МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Крымский федеральный университет имени В.И. Вернадского»

ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА БИЗНЕС-ИНФОРМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

II Международная научно-практическая конференция

«Проблемы информационной безопасности»

25-27 февраля 2016

Симферополь — Гурзуф

Проблемы информационной безопасности: сборник научных трудов II Международной научно-практической конференции, Гурзуф, 25-27 февраля 2016 / Под ред. д.т.н., профессора О.В. Бойченко. — Саки: ИП Бровко А.А., 2016. — 256 с.

Комитет конференции:

Председатель:
Бойченко Олег Валерьевич
д.т.н., профессор

Члены комитета:
Апатова Н. В., д.э.н., д.п.н., профессор
Герасимова С. В., д.э.н., профессор
Климчук С. В., д.э.н., профессор
Пенькова И. В., д.э.н., профессор
Цёхла С. Ю., д.э.н., профессор
Сигал А. В., д.э.н., доцент
Королёв О. Л., к.э.н., доцент
Иванов С. В., к.ф.-м.н., доцент
Акинина Л. Н., ст. преподаватель
Бакуменко М. А., ст. преподаватель

Подписано в печать 15.02.2016 г.
Формат 60x90 $^1/_8$. Бумага офсетная. Гарнитура Times New Roman.
Усл. п.л. 30,68. Количество экз. 150

Напечатано в ИП Бровко А.А.
296500 г. Саки, ул. Тимирязева, 30

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
кафедра бизнес-информатики и математического моделирования
Института экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КРИТЕРИИ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С распространением компьютерной сети Интернет во все сферы человеческой деятельности особое значение приобретает информационная безопасность данных, выставляемых пользователями сети различной степени открытости доступ. Киберпространство не имеет государственных границ, человек, осуществляемый несанкционированный доступ к компьютерной информации, может находиться на любой территории, автор компьютерного вируса может разместить его на популярном сайте и тем самым обеспечит его проникновение в различные страны. Данные условия, создающие информационные угрозы, требуют согласования законов и создание единого правового поля для информационной защиты в сети Интернет.

Одним из основных международных нормативных документов в данной сфере – это Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 года с Дополнительным протоколом о криминализации действий расистского и ксенофобского характера, реализуемые через компьютерные системы.

Большинство критериев уровня защищенности информации указаны в Британском стандарте BS 7799. Каждый пользователь Интернет или каждое предприятие для защиты своих информационных ресурсов должны нести определенные затраты. В России имеется ряд документов, наиболее поздние из них датированы 2008 годом, они содержат критерии информационной безопасности: ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель; ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности; ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

Среди критериев основными являются: конфиденциальность, целостность и доступность информации. Конфиденциальность – это сохранение в секрете информации, доступ к которой ограничен узким кругом пользователей. Целостность – свойство, согласно которому информация сохраняет свои первоначальные или согласованные с конечным пользователем вид и качество, нарушением целостности является санкционированное изменение содержания информации. Доступность – это использование информации по возможностям пользователя, имеющем соответствующие полномочия в необходимом для него виде, времени и месте, нарушение доступности влечет за собой невозможность получения или обработки информации.

К критериям оценки информационной безопасности следует отнести основные (доступность – устойчивость к отказу, использование ресурсов, обновление после сбоев, изменяемость; целостность – невозможность изменений, блокировки и уничтожения; конфиденциальность – доверие, официальность, сохранность, отсутствие скрытого доступа) и дополнительные (управляемость, релевантность, гарантия доставки и важность).

Для каждого критерия можно получить экспертную оценку или комплексную оценку в документации используемой информационной системы. В Интернет данные критерии должны применяться пользователями на всех этапах информационного взаимодействия.

УДК 004.01.04

Бойченко Олег Валерьевич
д.т.н., профессор
кафедра бизнес-информатики и математического моделирования
Института экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КОНТРОЛЬ НЕСАНКЦИОНИРОВАННОГО ВЛИЯНИЯ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МЕТОДОМ ТЕСТОВЫХ ИНТЕРФЕЙСОВ

Актуальность проведения исследований, связанных с разработкой новых методов и способов защиты данных информационных систем управления, обусловлена стремительным ростом внедрения процессов автоматизации в деятельность предприятий и организаций, как государственного сектора экономики, так и частных фирм и компаний.

Основным признаком таких систем является их открытость (технология OSI) в доступе к данным, обеспечивающим проведение рекламы для эффективного продвижения товаров и услуг, что предопределяет рентабельность и прибыльность деятельности предприятия.

С другой стороны, такой признак создает условия образования угрозы для коммерческой информации, а также персональных данных пользователей автоматизированной системы управления (АСУ) предприятия.

Современные подсистемы информационной безопасности ориентированы на создание барьера для защиты от угроз данных АСУ, что в основном обеспечивает достаточный уровень целостности, доступности и конфиденциальности информации.

Однако практический опыт свидетельствует о большом росте атак на компьютерные системы управления с применением новейших технических и программных средств и методов несанкционированного доступа к данным АСУ.

Так, согласно данным Cisco в 2015 году киберпреступники изрядно осмелели и все активнее внедряются в веб-ресурсы путем кражи данных и доступа к серверам АСУ. Это создало условия для роста уязвимостей подделки межсайтовых запросов (CSRF), несмотря на то, чсто с 2014 по 2015 год категория межсайтового скриптинга (XSS) сократилась на 47 % [1].

Анализ также показывает, что организации достигли определенных успехов в шифровании информации при передаче между узлами, однако хранимые данные нередко остаются незащищенными.

В большинстве значимых нарушений безопасности за последние несколько лет злоумышленники воспользовались незашифрованными данными, хранящимися в центре обработки данных и других внутренних системах, что позволило хакерам добираться до ценных сведений без особых проблем.

Одной из актуальных проблем информационной безопасности является то, что авторы некоторых вариантов программ-вымогателей, а также другие разработчики, использующие уязвимости, теперь переносят трафик на взломанные веб-сайты с WordPress.

Это усложняет обнаружение и дает возможность воспользоваться пространством на сервере. Интернет полон заброшенных сайтов, созданных с помощью WordPress, за информационной безопасностью которых никто не следит. Такие сайты нередко взламывают и используют для осуществления атак.

Так, с февраля по октябрь 2015 года число доменов WordPress, используемых преступниками, выросло на 221 % (рис. 1), чему способствовало то, что взломанные сайты WordPress часто работали не на последней версии WordPress, отличались слабыми паролями администратора и использовали подключаемые модули без исправлений информационной безопасности.

На основании исследования данных Cisco [2], следует выделить основные типы программного обеспечения (ПО) и файлов, чаще всего размещаемые на взломанных сайтах WordPress:

- исполняемые файлы, представляющие собой информационное наполнение для атак с использованием комплектов эксплойтов;
- файлы конфигурации для вредоносного ПО (Dridex, Dyre);
- прокси-код, передающий данные для сокрытия инфраструктуры управления и контроля;
- фишинговые веб-страницы для сбора имен пользователей и паролей;
- сценарии HTML, перенаправляющие трафик на серверы;
- комплекты эксплойтов.

Рис 1. Динамика роста числа доменов WordPress за 2015 год, %

Отличительной характеристикой использования взломанных сайтов WordPress является также создание вредоносной инфраструктуры, такой как Dridex, Necurs (ПО для кражи информации), Pony (ПО для кражи паролей), TeslaCrypt, Cryptowall 3.0, TorrentLocker (программы-вымогатели), Andromeda (ботнет для рассылки спама), троянских дропперов Bartallex, а также фальшивых страниц входа.

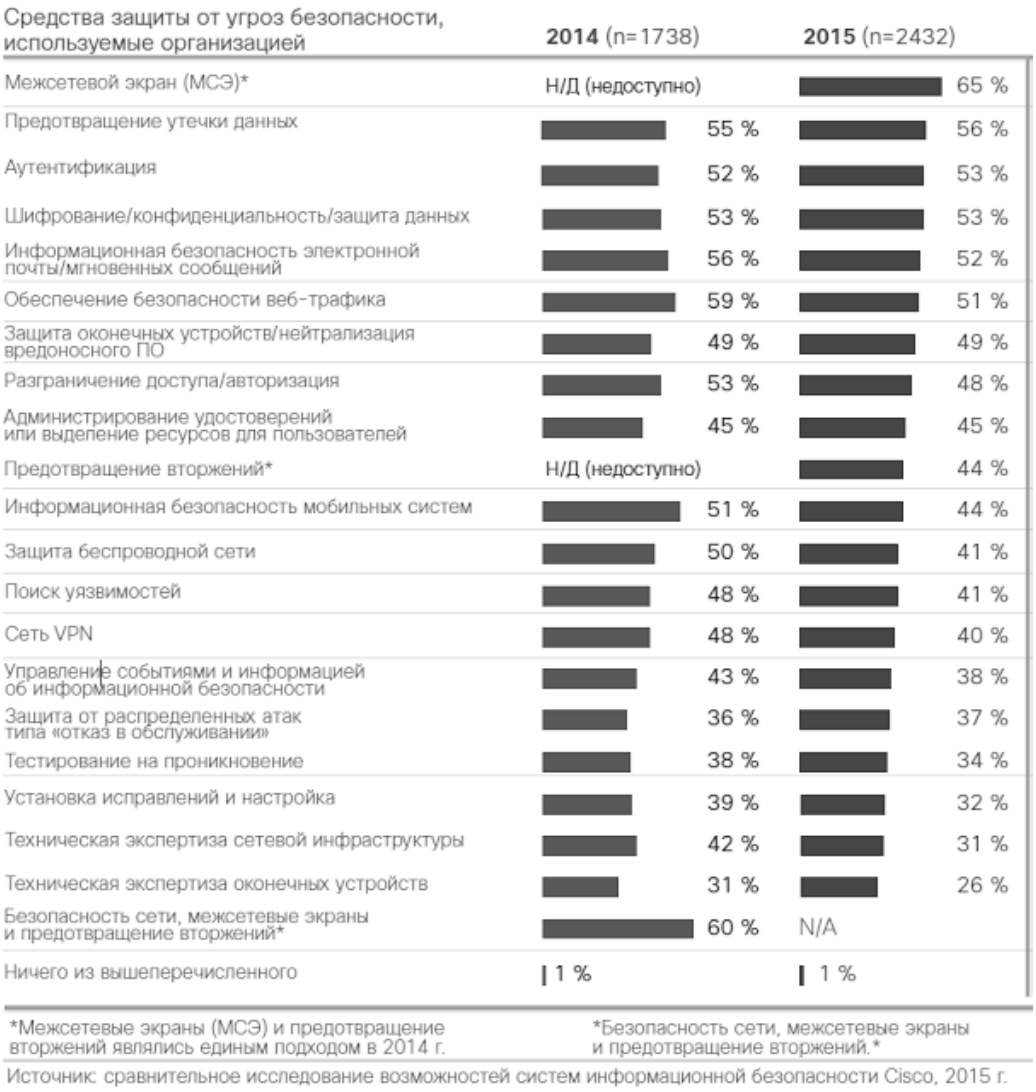
Последующий анализ современной практики информационной безопасности позволил выделить межсетевой экран в качестве наиболее популярного средства защиты данных АСУ (Рис. 2).

Однако, анализ показывает, что действия злоумышленников по несанкционированному доступу к данным информационных систем управления и корпоративным сетям становятся все более изощренными (использование вредоносного рекламного и шпионского ПО, программ нежелательного перенаправления, эксплойтов iFrame, программы фишинга и др), как показано на рис. 3.

По анализу опроса ИТ-руководителей организаций и предприятий установлено, что наибольшей внешней проблемой информационной безопасности за 2015 год является вредоносное ПО 68 %, а фишинг и сложные целенаправленные угрозы заняли второе и третье место – 54 % и 43 % соответственно.

Что касается внутренних проблем информационной безопасности, то более половины (54 %) респондентов как основную угрозу указали загрузки вредоносного ПО, а также внутренние нарушения сотрудниками (47 %) и уязвимости аппаратного обеспечения и ПО (46 %).

Особую опасность в части проблематики информационной безопасности корпорации представляют сетевые DDoS-атаки SSHPsychos, на которые в отдельные моменты времени на SSHPsychos приходилось свыше 35 % всего мирового трафика SSH в Интернете.



Средства защиты от угроз безопасности, используемые организацией	2014 (n=1738)	2015 (n=2432)
Межсетевой экран (МСЭ)*	Н/Д (недоступно)	65 %
Предотвращение утечки данных	55 %	56 %
Аутентификация	52 %	53 %
Шифрование/конфиденциальность/защита данных	53 %	53 %
Информационная безопасность электронной почты/мгновенных сообщений	56 %	52 %
Обеспечение безопасности веб-трафика	59 %	51 %
Защита оконечных устройств/нейтрализация вредоносного ПО	49 %	49 %
Разграничение доступа/авторизация	53 %	48 %
Администрирование удостоверений или выделение ресурсов для пользователей	45 %	45 %
Предотвращение вторжений*	Н/Д (недоступно)	44 %
Информационная безопасность мобильных систем	51 %	44 %
Защита беспроводной сети	50 %	41 %
Поиск уязвимостей	48 %	41 %
Сеть VPN	48 %	40 %
Управление событиями и информацией об информационной безопасности	43 %	38 %
Защита от распределенных атак типа «отказ в обслуживании»	36 %	37 %
Тестирование на проникновение	38 %	34 %
Установка исправлений и настройка	39 %	32 %
Техническая экспертиза сетевой инфраструктуры	42 %	31 %
Техническая экспертиза оконечных устройств	31 %	26 %
Безопасность сети, межсетевые экраны и предотвращение вторжений*	60 %	N/A
Ничего из вышеперечисленного	1 %	1 %

*Межсетевые экраны (МСЭ) и предотвращение вторжений являлись единым подходом в 2014 г.

Безопасность сети, межсетевые экраны и предотвращение вторжений.

Источник: сравнительное исследование возможностей систем информационной безопасности Cisco, 2015 г.

Рис. 2. Средства защиты от угроз, используемые организацией

Рис. 3. Наиболее распространенное вредоносное ПО

Все большей значимости приобретает проблема обновления ПО компании.

Так, в частности установлено, что некоторые клиенты Cisco в области финансовых услуг, здравоохранения и розничной торговли используют версии программного обеспечения Cisco, выпущенные более 6 лет назад (Рис. 4).

Понятно, что в такой ситуации создаются дополнительные благоприятствующие условия для создания уязвимостей к данным АСУ.

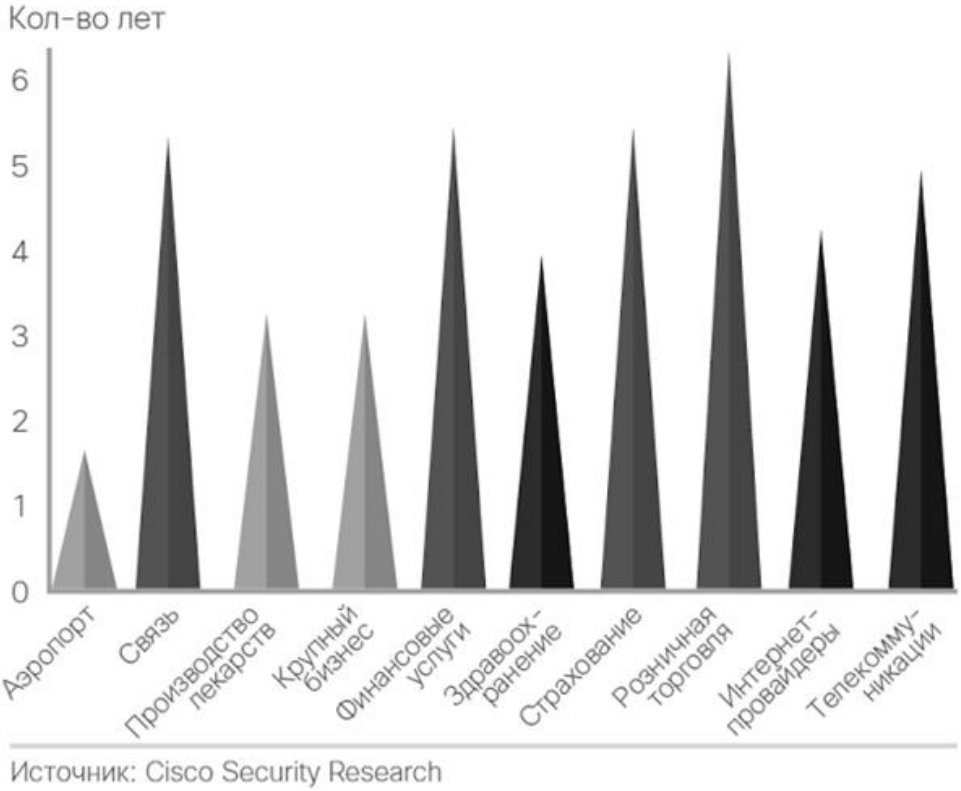


Рис. 4. Средний возраст программного обеспечения в годах

В такой ситуации целесообразным является разработка нового метода для выявления несанкционированного влияния на ПО АСУ.

Соответственно методологии структурного проектирования, каждая проектируемая задача разбивается на два компонента: функциональный (ядро) и интерфейс для связи ядра с системой через операционную систему (ОС) [3]. Ядро выполняет продиктованные задачи функции и оформляется в виде подпрограммы, руководство которой передается с интерфейса [4]. С помощью интерфейсов между ядрами устанавливаются связи по управлению (через ОС) и по данным (через базу данных, общую часть или некоторые другие средства). Интерфейсы, используемые в процессе нормальной эксплуатации, назовем рабочими интерфейсами (РИ) [5, 6]. РИ получает управление от ОС и вызывает на работу ядро, с передачей ему необходимых данных. После отработки ядра управление возвращается на РИ, а результаты расчета (исходные данные ядра) передаются РИ по назначению. Управление через ОС передается следующей задаче (следующему РИ). Структура задачи ядро-интерфейс позволяет организовать тестирование ядра (в процессе проектировки) методом тестового обрамления. Суть метода состоит в использовании специального тестового интерфейса (ТИ). ТИ содержит входные наборы для проверки маршрутов ядра и входные эталонные наборы. Предусматривается использовать ТИ для контроля целостности ядер в процессе нормальной эксплуатации. В ядро задачи закладываются средства фиксации маршрута прохождения обработки данных на реальном наборе данных (практически в каждую ветку программы ставится счетчик, а вектор счетчиков доступен ТИ). Ядро запускается на выполнение через РИ. Результаты работы временно запоминаются в РИ. ТИ по значениям вектора счетчиков определяет ветку прогона и повторно запускает ядро с тестовым набором данных для этого маршрута (рис. 5). Данные отработки сравниваются с эталонными.

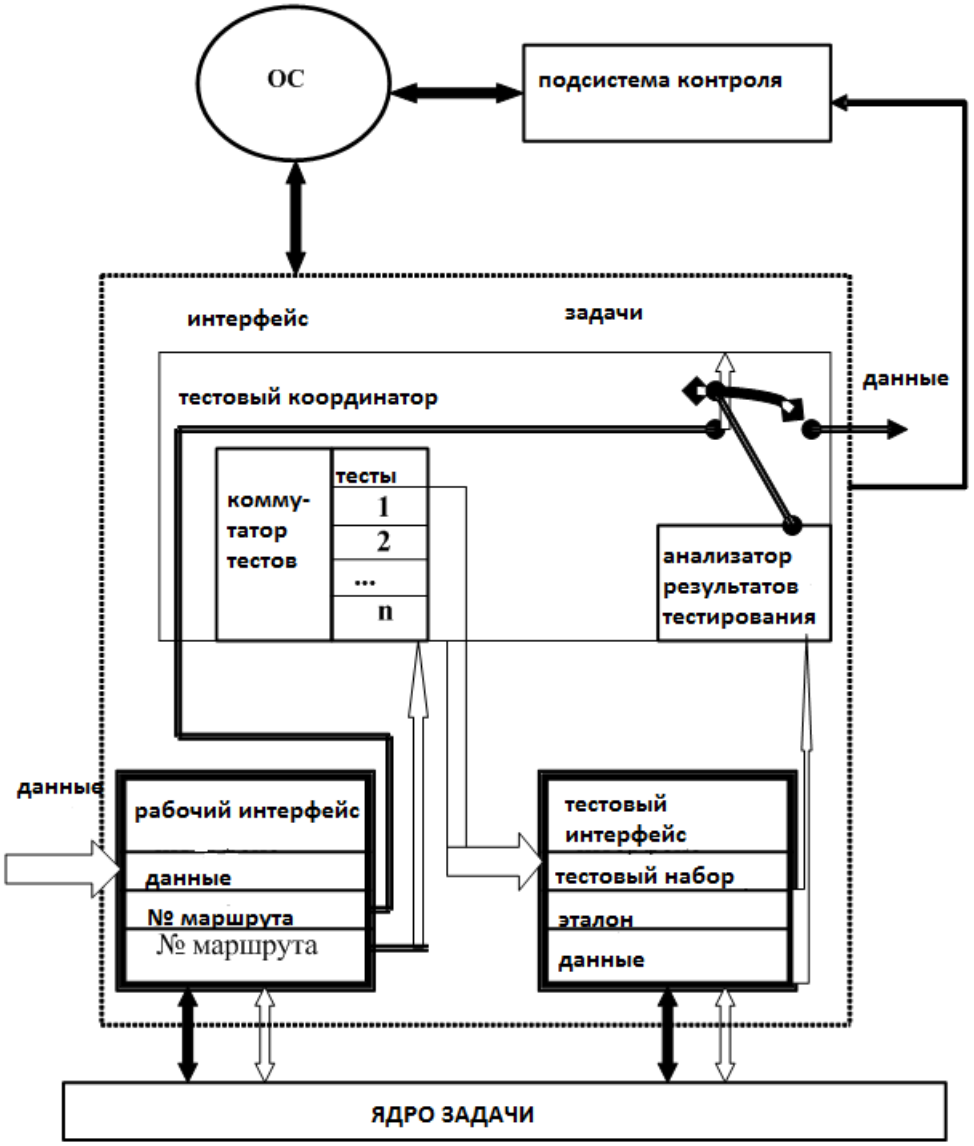


Рис. 5. Схема организации интерфейса задачи

В случае совпадения («тест прошел») с РИ выдаются результаты первого прогона. В противном случае главная задача системы, которая выполняет функции подсистемы контроля, оповещается о «неисправности» ядра и результаты первого прогона считаются недействительными.

На рис. 6. изображен алгоритм, выбранный для иллюстрации схемы ядра. На рис. 7 изображен граф, который соответствует ядру.

В точках программы, которые отвечают вершинам графовой модели, устанавливается занесение 1 в соответствующие ячейки тестового счетчика программы, а в точке, которая отвечает вершине с номером i (для данного примера $i = 1,2,...6$) 1 заносится у i-й бит значением вектора счетчиков. Точно также определяются и остальные предикаты модели.

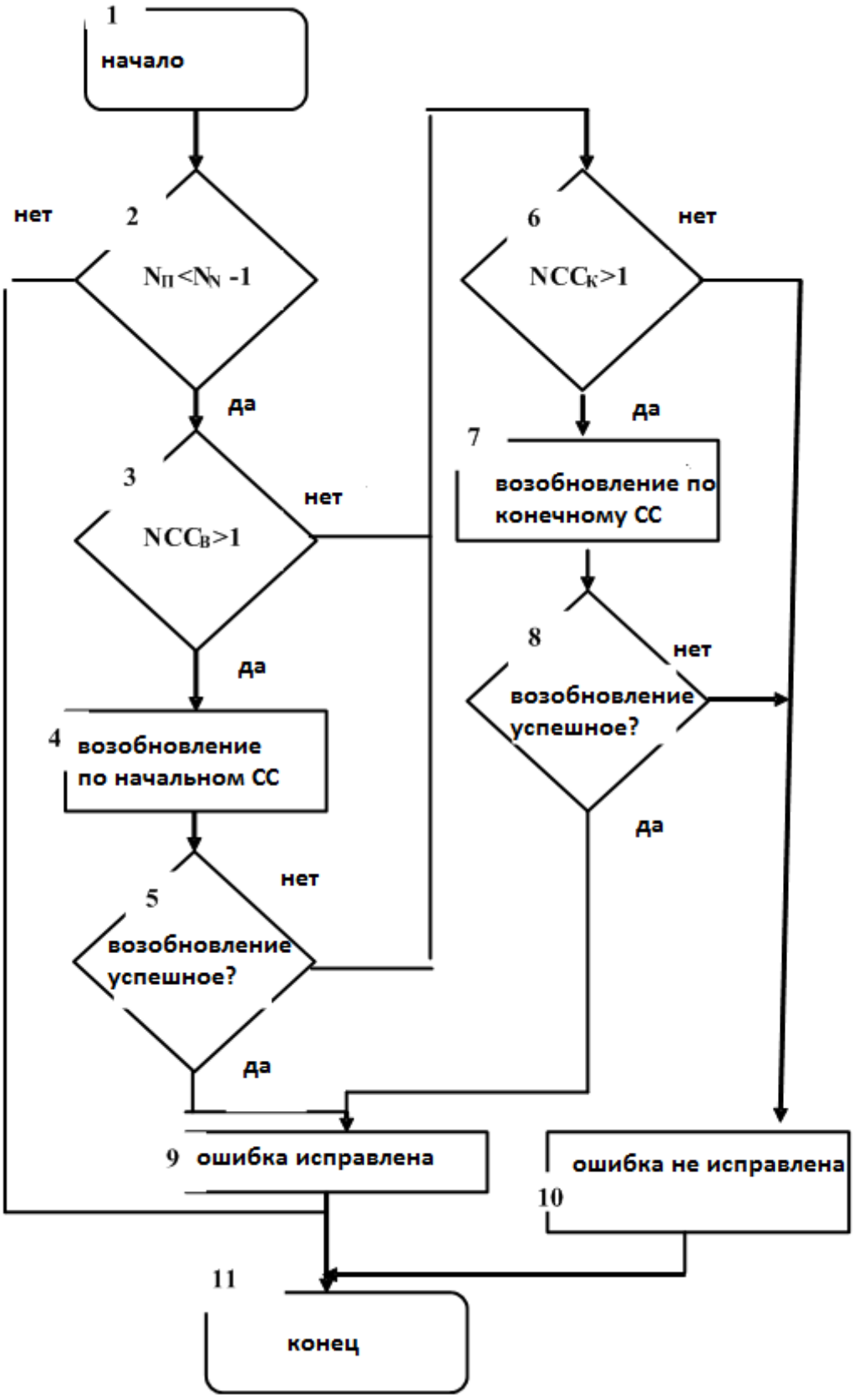


Рис. 6. Схема ядра

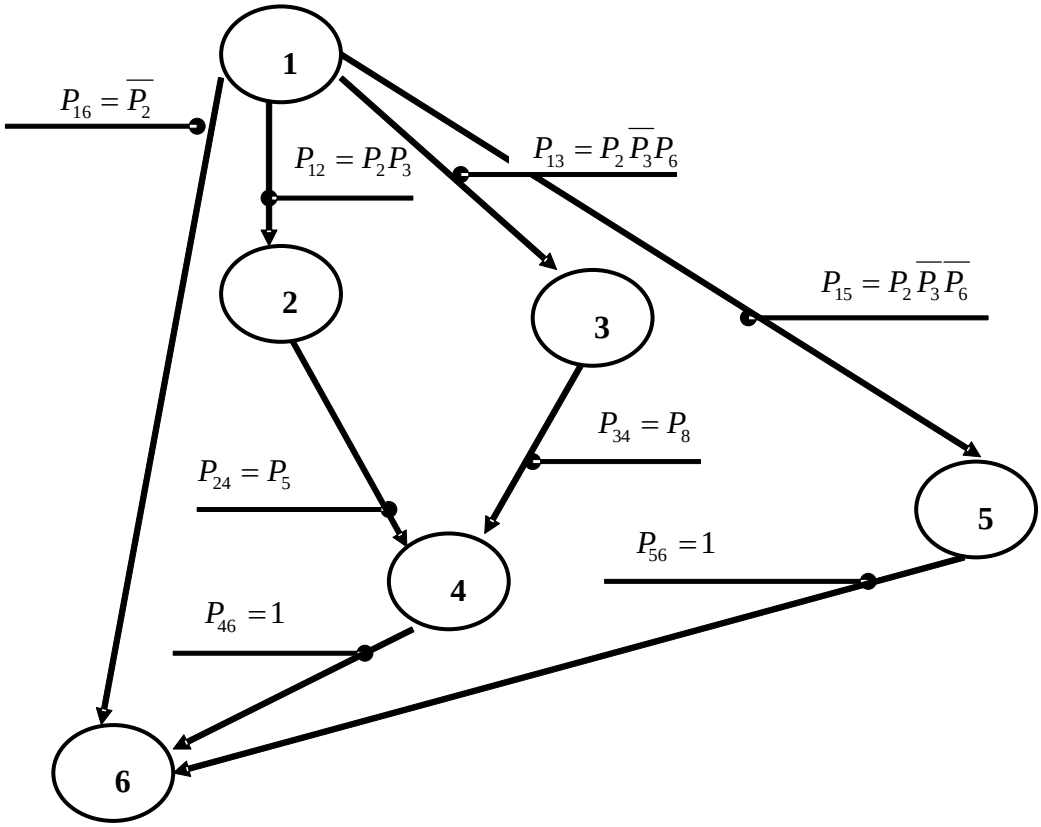


Рис. 7. Графовая модель программы-ядра:

P_2 - предикат типа $N_{\Pi} \langle N_N - 1$.

$\overline{P}_2$ - предикат типа $N_{\Pi} \rangle = N_N - 1$.

P_3 - предикат типа $NCC_B \rangle 1$.

$\overline{P}_3$ - предикат типа $NCC_B = \langle 1$.

После первого прогона на реальных данных значения счетчика тестового набора для проверки дееспособности (неповрежденности) данного ядра в нужных именно сейчас ветках.

В результате обеспечения устойчивости на уровне макроструктуры реализуется средствами организующей системы, которая позволяет выявлять и обрабатывать ошибки и отказы устройств ввода-вывода (УВВ) при обмене, превышение допустимого времени реакции УВВ на запрос процессора, обращение к защищенным участкам памяти (нарушение адресации), ошибки прерывания схем контроля процессора, ошибки при чтении (записи) информации с внешней памяти, обращение к ресурсу, отсутствующему в системе, а также обращение к неисправному УВВ, дисплею и ошибки в вызове супервизора ОС в командах оператора.

Таким образом, в результате проведенных исследований предложен метод тестовых интерфейсов, обеспечивающий создание условий для организации контроля и возобновления работы системы путем предоставления пользователю следующих видов услуг:

- развитый аппарат контрольных точек;
- коды завершения, которые идентифицируют результаты работы при окончании всех операций с УВВ и псевдоустройствами;
- переход на исправный процессор без вмешательства (или при минимальном вмешательстве) при выходе из строя одного из процессоров в многопроцессорной АСУ;
- принудительное завершение выполнения задач с программы пользователя;

- реализация распечатки диагностических сообщений для оператора с указанием кодов завершения, состояния процессора, имени задачи, при выполнении которой состоялось выявление ошибки;
- разрешение пересылки данных между разделами;
- допуск резервирования разделов ОЗУ;
- открытость для наращивания дополнительными модулями (агрегативность).

Список литературы:

1. Клаверов В.Б. Проблемы противодействия компьютерной преступности / Клаверов В.Б. [Электронный ресурс]. – Режим доступа: http: // www.securitylab.ru / contest / 382194.php.
2. Павлов А. В. Отчет Cisco за 2015 год: зачем ломают сайты на WordPress и какие атаки стали использовать чаще / А.В. Павлов [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/479100.php
3. Сбітнєв А.І. Структурне проектування спеціального програмного забезпечення / А.І. Сбітнєв, С.В. Ленков, О.М. Грищак // Вісник Східноукраїнського національного університету ім В. Даля. – Луганськ: СНУ, 2007. – Ч. 1. – № 5 (111). – С. 147-154.
4. Сбитнев А. И. Структурные методы проектирования математического обеспечения АСУ ТП / А.И. Сбитнев // Модели и алгоритмы автоматизированных систем в промышленности. – К.: ИК АН УССР, 1982. – С. 3-9.
5. Пайк Х. Разработка программного обеспечения для мини-ЭВМ / Х. Пайк // Мини-ЭВМ. – М.: Мир, 1975. – С. 27-41.
6. Бойченко О.В. Структурне проектування програмного забезпечення складних інформаційних систем реального часу / О.В. Бойченко С.В. Лєнков, П.А. Шкуліпа // Сучасна спеціальна техніка. – К.: ДНДІ МВС України, 2012. – № 4(31). – С. 92-97.

УДК 330

Борщ Людмила Михайловна
д.э.н., профессор
кафедра финансов предприятий и страхования
Института экономики и управления
ФГАОУ ВО «Крымский федеральный университет
им. В.И. Вернадского»
Республика Крым, Россия

ВОЗДЕЙСТВИЕ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Современное развитие экономической системы невозможно представить без инвестиций. В экономическом развитии страны инвестиции выполняют ведущую роль по достижению экономического роста, изменении структуры капитала, что существенно влияет на уровень жизни, стабильности и повышению конкурентоспособности.

В исследовании раскрыты теоретические положения государственного регулирования инвестиционной деятельности, выполняющие ведущую роль в достижении экономического роста, изменении структуры капитала, повышенного уровня жизни и макроэкономической стабильности. Предложены методы государственного регулирования инвестиционной деятельности через механизмы воздействия на экономику и социальные процессы, устраняя диспропорции и гармонизируя их стабильное развитие. Объектом инвестиционной деятельности является общественные отношения относительно государственное регулирование относительно влияния на формирование инвестиционных источников и форм модернизации экономики.

Предметом исследования являются организационно управленческие механизмы обеспечение воспроизводственных процессов.

Необходимость координации стимулирования субъектов управления инвестициями их активизации объясняется не только действиями кредиторов, ищущих прибыльных инвестиционных возможностей, но и появлением технических усовершенствований и нововведений. Массовое обновление средств производства, продиктованное необходимостью снижения издержек для повышения прибыли, служит

одновременно как основным фактором выхода из текущего кризиса, так и причиной диспропорций, которые порождают будущие кризисы. Текущее состояние инвестиционной сферы в России таково, что даже при самых благоприятных тенденциях мировой конъюнктуры невозможно достичь прорыва ни в технологической, ни в структурной перестройке без целенаправленных усилий государственной инвестиционной политики.

Для координации стимулирования субъектов управления инвестиционной деятельности необходимо учитывать, какие именно факторы влияют на принятие инвестиционных решений, и каким образом государство может влиять на эти факторы. Эластичность спроса и предложения инвестиционных фондов по основным детерминантам инвестиционной деятельности, равно как и проблема инвестиционных лагов служит основой государственной инвестиционной политики.

Кризисное развитие экономики с введением санкций показало, что государственное стимулирование инвестиций должно осуществляться с помощью комплексной системы мер как бюджетно-налоговой, так и кредитной и денежной политик.

Координация и стимулирование наиболее действенных механизмов инвестиционной деятельности должно служить важным фактором обеспечения устойчивого роста и позволит выйти из кризисного состояния российской экономики.

Сложность государственного регулирования в инвестиционной сфере российской экономики связаны с ослаблением системы государственного управления в условиях несформированных рыночных механизмов, усиливающих эффективность рыночного управления внутренними и внешними денежными потоками по обеспечению повышения экономической роли государства в развитии страны.

Инвестиционная деятельность на микро- и макроэкономическом уровне всегда связана с процессом инвестирования экономических ресурсов. Учитывая тот фактор, что на микроэкономическом уровне определяется будущие экономические возможности хозяйствующих субъектов, на макроэкономическом уровне определяются будущие возможности государства по созданию социально-экономических услуг обществу.

На макроэкономическом уровне инвестирование рассматривается как процесс государственной поддержки хозяйственных субъектов по вложению в производство или социальные объекты экономических ресурсов. Инвестиционная деятельность на макроэкономическом уровне связана с регулированием процесса инвестирования. Регулирование инвестиционной деятельности со стороны государства направлено на стимулирование инвестиционного спроса и предложения, также может быть направлено на сдерживание инвестиционной активности.

Государство в регулировании инвестиционной деятельности принимает участие в зависимости от состояния экономики страны (стадии цикла, дефицитности государственного и региональных бюджетов, уровня инфляции, возможности мобилизовать финансовые ресурсы внутри страны) применяются концепции регулирования. В зависимости от состояния экономики применяются концепции двухуровневой системы: во-первых, увеличение валового внутреннего продукта, роста объема производства и реализации продукции, роста занятости населения, снижение темпов инфляции, повышения общего благосостояния населения; во-вторых, соотношение между инвестиционным спросом и предложением на капитал, динамикой денежной массы, процентных ставок, курса национальной валюты.

Государственное регулирование инвестиционной деятельности осуществляется напрямую через государственный сектор экономики, так и опосредовано – институциональную систему (органов исполнительной власти, органов исполнительной власти субъектов федерации и местного самоуправления, а также различные финансово-экономические, денежно-кредитные и организационно-управленческие институты), которые влияют на инвестиционный процесс на макро- и микроэкономическом уровне.

Государство всегда осуществляет инвестиционное регулирование в экономическом секторе в соответствии с определенной инвестиционной политикой, выраженной

комплексом правовых, административных и экономических действий государства, направленных на расширение и активизацию инвестиционных процессов. На активизацию инвестиционных процессов авторы «Стратегии 2020» предлагают создать при правительстве Национальный совет по инвестициям и контроля норм для повышения эффективности нормативно-правового регулирования предпринимательской активности. Целью государственной политики России является создание конкурентной среды, реализация программ структурированной перестройки экономики.

Соответственно можно встретить самые различные определения инвестиционной политики в экономической литературе, так Борисов А.Б. в «Большом экономическом словаре» дает такое определение: «Инвестиционная политика – составная часть экономической политики, проводимой государством и предприятиями в виде установления структуры и масштабов инвестиций, определения направлений их использования, источников получения учетом необходимости обновления основных средств и повышения их технического уровня» [1; с. 273]. Несколько по другому суть государственного инвестиционного регулирования излагается автором в более ранних изданиях: «Государственное регулирование инвестиционной деятельности – это целенаправленная деятельность государства по обеспечению благоприятных условий для осуществления инвестирования с целью эффективного использования инвестиционного потенциала в целях подъема экономики увеличения ВНП и социально-экономического развития с переходом на новый технологический уклад» [2; с. 103]. Более точное определение государственного регулирования приводит Герасимова С.В.: «Государственное регулирование – это часть общей экономической политики государства, направленной на содействие привлечения инвестиций посредством развития социальной и экономической сферы и осуществляется в соответствии с законодательством» [3; с. 397].

Таким образом, в экономической литературе существуют различные взгляды как на государственную инвестиционную политику и государственное регулирование инвестиционной деятельности, так и на методы государственного регулирования инвестиционной деятельности, и составляют важную часть повышения эффективности инвестиционного процесса в реальном секторе экономики.

Обосновывая необходимость оптимизации государства в инвестиционном развитии через государственное регулирование, рассмотрим методы государственного регулирования инвестиционной деятельности (рис. 1).

Финансовые методы являются методами регулирования через механизм воздействия на экономику и социальные процессы, устраняя диспропорции и гармонизируя процессы стабильного развития, внедряя передовые технологии. Следовательно, в основе государственного регулирования заложены специфические финансовые методы, которые составляют основу государственного регулирования.

Государственное регулирование обеспечено через совокупность способов и приемов достижения целей инвестиционной деятельности, основанных на денежных отношениях по поводу распределения и перераспределения ВВП и части национального богатства для формирования и эффективного использования финансовых ресурсов.

Следует отметить, что Российская Федерация за последние годы приложила значительные усилия для улучшения инвестиционного климата внутри страны. Так, инвестиции в основной капитал 2005-2014 гг. отражены на рисунке 2.

Инвестиции в основной капитал с 2005 года возросли на 9916574,7 млрд руб или в 3,7 раза. По данным на 31 декабря 2013 года по объему накопленных иностранных инвестиций Россия находилась на 16 месте в мире.

Государственной регулирования инвестиционной деятельности осуществляется на базе двух принципов: прямого участия в инвестициях (создание условий), стимулирующую инвестиционную деятельность и косвенного. Прямое участие в инвестициях, по мнению автора, должно осуществляться по принципу. Основная часть федеральных инвестиционных средств должна поддерживать фундаментальные: государственные, социально-экономические программы, определяющие первоочередные

задачи по развитию высокотехнологической экономики, затрачивая те сектору [4; с. 140].

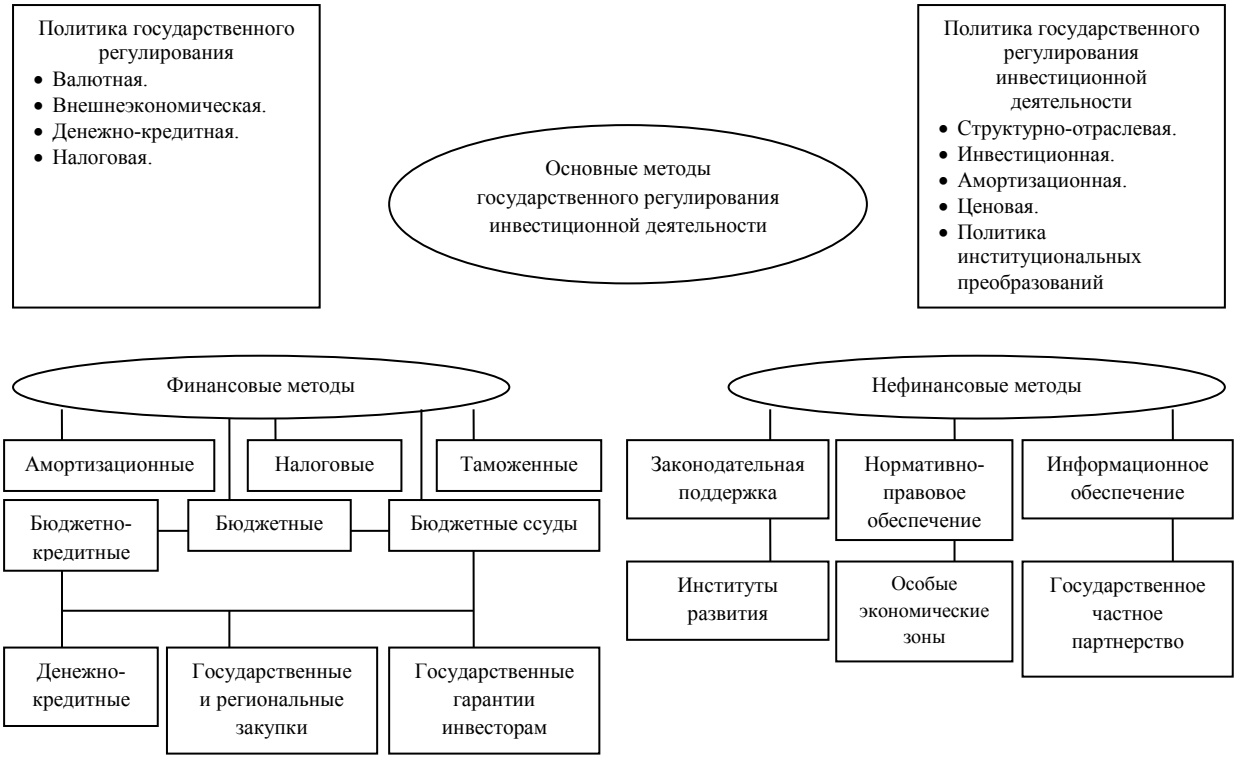


Рис. 1. Методы государственного регулирования инвестиционной деятельности*

* Разработано и составлено автором

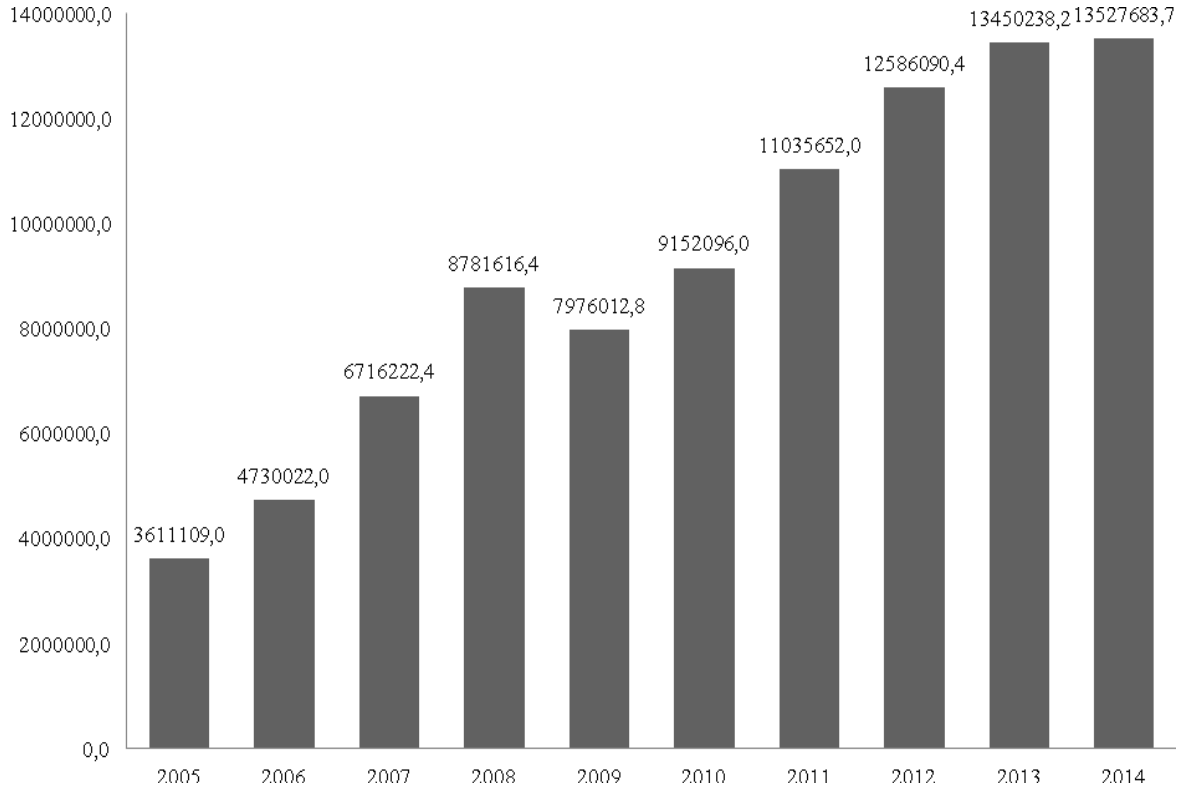


Рис. 2. Инвестиции в основной капитал Российской Федерации, млрд. руб.*

* Построено автором согласно данных Министерства экономического развития Российской Федерации [5]

Следующим принципом является необходимость разработать инвестиционную концепцию регионов, предусматривающую набор альтернатив за счет инвестиций. Такая модель, составленная в регионах, должна иметь следующие важнейшие составляющие: обоснованные идеи и критерии выработки системы приоритетов регионального развития. Необходимо также обосновать определенные формы организационно-экономического механизма инвестирования через такие принципы как: принцип мониторинга и анализа инвестиционной деятельности в регионе, принцип разработки инвестиционной политики с учетом кластеров и регионов, принцип реализации государственного регулирования инвестиционной деятельности, активизируя инвестиционный процесс на региональном уровне.

Выводы:

В результате исследования обоснованы результаты, которые в совокупности решают макроэкономическую проблему государственного регулирования инвестиционных воспроизводственных процессов экономики.

В современных условиях на основании определенной цели первоочередными задачами государства и органами исполнительной власти должны определятся первоочередные эффективные направления реализации инвестиционной1 политики, устранение преград для минимизации рисков.

Эффективность инвестиционной деятельности отраслей экономики определяется результатом хозяйственной деятельности отраслей, их техническим уровнем, организацией производства, уровнем предпринимательской активности, способностью внедрения инноваций на всех этапах воспроизводственного цикла.

Основными направления инвестиционной деятельности должно быть улутшение воспроизводственной структуры капиталовложений, повышение части затрат на техническое перевооружение и реконструкцию действующих хозяйственных субъектов.

Центр весов государственной инвестиционной деятельности должен переместится на региональный уровень, эффективной формой должно быть двухстороннее финансирование инвестиционных проектов.

Государственная политика направлена на инвестиционное регулирование в экономическом отраслевом секторе в соответствии с определенной инвестиционной политикой, выраженной комплексом правовых, административных и экономических действий государства, направленных на расширение и активизацию инвестиционных процессов в государстве.

Список используемых источников

1. Большой экономический словарь : [более 20000 терминов] / авт. и сост. А.Б. Борисов. – Изд. 2-е, перераб. и доп. – М.: Книжный мир, 2005. – 860 с.

2. Борщ Л.М. Ипотечное кредитование в системе финансовой безопасности банков / Л.М. Борщ // Научный вестник: финансы, банки, инвестиции. – 2014. - № 3(28). – С. 106-113.

3. Борщ Л.М., Герасимова С.В. Інвестування: теорія і практика: Навч. посіб. – 2-ге вид., перероб. і доп. – К.: Знання, 2007. – 685 с. (Вища освіта ХНІ століття). (Рекомендовано Міністерством освіти і науки. Лист № 14/18.2-1585 від 01.07.2004 р.).

4. Финансовые и денежно-кредитные методы регулирования экономики. Теория и практика : учебник для магистров / Финансовый университет при Правительстве Российской Федерации ; под ред. М.А. Абрамовой, Л.И. Гончаренко, Е.В. Маркиной. – Москва: Юрайт, 2014. – 551 с.

5. Справка об инвестициях [Электронный ресурс] / Официальный сайт Министерства экономического развития Российской Федерации. – Режим доступа: http://www.economy.gov.ru.

Волочко Александр Тихонович
д.т.н., профессор
Зеленин Виктор Алексеевич
д.т.н., профессор
Нарушко Елена Олеговна
аспирант
Физико-технический институт НАН Беларуси
Минск, Беларусь

МНОГОСЛОЙНЫЕ ПОКРЫТИЯ НА ЭЛЕМЕНТАХ КОМПЬЮТЕРА КАК СРЕДСТВО ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Неуклонный рост числа и быстродействия электронных объектов приводит к повышению электромагнитного фона в окружающем нас мире. Немало устройств излучают электромагнитные волны (ЭМВ), которые оказывают воздействие на живые организмы, вносят изменения в работу особо чувствительных измерительных приборов, сильно усложняя получение достоверных данных. Электромагнитные излучения (ЭМИ) элементов компьютера могут послужить одним из каналов утечки информации. Принимая и декодируя их сигналы, можно получить информацию о базе данных компьютера, внести изменения и нарушить его работу. Для защиты от несанкционированного доступа все электронные системы и компьютеры должны иметь эффективные экранирующие покрытия, наносимые на поверхности пластмассового корпуса, а дисплей, обладая способностью экранирования электромагнитных волн, одновременно должен давать возможность оператору видеть отображаемую на нем информацию, чем обусловлена необходимость получения прозрачных защитных покрытий.

В связи со сложившейся задачей по надежной защите элементов электронных объектов, прежде всего дисплеев, которые, как правило, состоят из пластикового корпуса и стеклянного экрана, нами были разработаны два вида покрытий.

Первый вид, предназначенный для защиты корпуса компьютера, представлял собой многослойные покрытия, состоящие из периодически чередующихся диамагнитных высокоэлектропроводящих и ферромагнитных слоев заданного состава с различной толщиной каждого отдельного слоя, наносимых на полимерные подложки. Известно, что слои из материалов с высокими значениями относительной магнитной проницаемости (пермаллой, электротехническая сталь, супермаллой и др.) хорошо поглощают ЭМИ в диапазонах частот 0,1 – 10 кГц и выше 1 МГц, замыкая линии магнитного поля через толщу ферромагнитной пленки [1-3]. При частотах от 0,1 до 1 МГц, где величина потерь ЭМИ за счет механизма отражения преобладает над величиной потерь за счет механизма поглощения, эффективно использование высокоэлектропроводящих слоев (Cu, Ag) [4].

Другой вид покрытий, предназначенных для защиты от ЭМИ прозрачных элементов компьютера (монитор, дисплей), представлял собой конструкцию, состоящую из чередующихся металлических и диэлектрических слоев. В качестве металлической составляющей были использованы высокоэлектропроводящие металлы (Cu, Ag, Au), в качестве диэлектриков – оксиды, имеющие высокий показатель преломления (TiO_2,SiO_2, ZrO_2).

В результате проведённых расчётов и экспериментов наилучшими экранирующими ЭМИ оказались покрытия 100Cu/300Ni80Fe20 (где 100 и 300 – толщины слоев меди и пермаллоя, в нм) – для корпуса электронного объекта (рис.1. а) и $45ZrO_2$/5Ni/$45ZrO_2$/22Cu/2Ni/$45ZrO_2$ – для дисплея (рис.1. б) [4,5].

Рис. 1. Изображение защищенных элементов компьютера:
а – корпуса монитора и клавиатуры; *б* – монитор компьютера

Покрытия 100Cu/300Ni80Fe20 и $45ZrO_2$/5Ni/$45ZrO_2$/22Cu/2Ni/$45ZrO_2$ были получены электронно-лучевым методом на установке ВУ - 1Б. Данный метод позволяет наносить широчайший спектр материалов, включая металлы, сплавы, оксиды, нитриды, всевозможные многослойные композиционные покрытия вследствие широкого диапазона изменения энергии электронного луча. Преимущество электронно-лучевого испарения заключается в том, что в отличие от, например, магнетронного распыления, магнитные свойства испаряемых материалов (железо-никелевые сплавы-Ni80Fe20), не влияют на скорость испарения покрытий. Для контроля оптических характеристик покрытий была использована система контроля на базе спектрометра EOS45 – серии IRIS, встроенная в вакуумную установку ВУ – 1А, что позволило контролировать процесс нанесения с точностью до 1 нм толщины наносимого покрытия.

Эффективность экранирования полученных таким образом покрытий 100Cu/300Ni80Fe20 и $45ZrO_2$/5Ni/$45ZrO_2$/22Cu/2Ni/$45ZrO_2$ для радиочастотного диапазона длин волн (100 МГц-10ГГц) достигает 45-50 дБ и 30-35 дБ соответственно. Пропускание света *T* для покрытия монитора не менее 60 %, отражение *R* – не более 2-3 %, поверхностное электросопротивление $\rho \approx 2$ Ом/кв [5].

Адгезионные свойства покрытий были исследованы с помощью Scratch Tester JLST022. Метод основан на контролируемом царапании индентором с радиусом закругления R=200 мкм [6] выбранного участка образца. При этом вертикальная нагрузка и максимальная сила трения изменяются в пределах от 0 до 200 Н. Скорость увеличения нагрузки составляет 10 Н/мин, максимальная длина пути - 70 мм при скорости движения индентора от 0,4 до 600 мм/мин и максимальной глубине внедрения в покрытие до 1 мм с разрешением по глубине ~1,5 нм. В наших испытаниях алмазный наконечник иглы перемещался по поверхности образца с возрастающей нагрузкой, при этом фиксировались параметры нагрузки, сила трения, глубина проникновения индентора, а также сигналы акустической эмиссии (рис.2).

Для покрытия 100Cu/300Ni80Fe20 рис.1 а характерно его вдавливание в мягкий материал подложки из поликарбоната. При это покрытие теряет сплошность, но тем не менее держится на основании. Что касается покрытия 100Cu/300Ni80Fe20 на стекле, то здесь наблюдается полное отделения пленки, даже при нагрузке в 1,94 Н. Данный эффект может объясняться плохой адгезией меди к стеклу. Для образца с покрытием $45ZrO_2$/5Ni/ZrO_2/22Cu/2Ni/$45ZrO_2$ на стеклянном основании скольжение индентора до нагрузки 14 Н происходило без видимых изменений. При увеличении нагрузки от 14,08 до 19,83 н происходило частичное скалывание пленки, а при нагрузке 19,83-25,00 наблюдалось ее процарапывание вплоть до материала подложки.

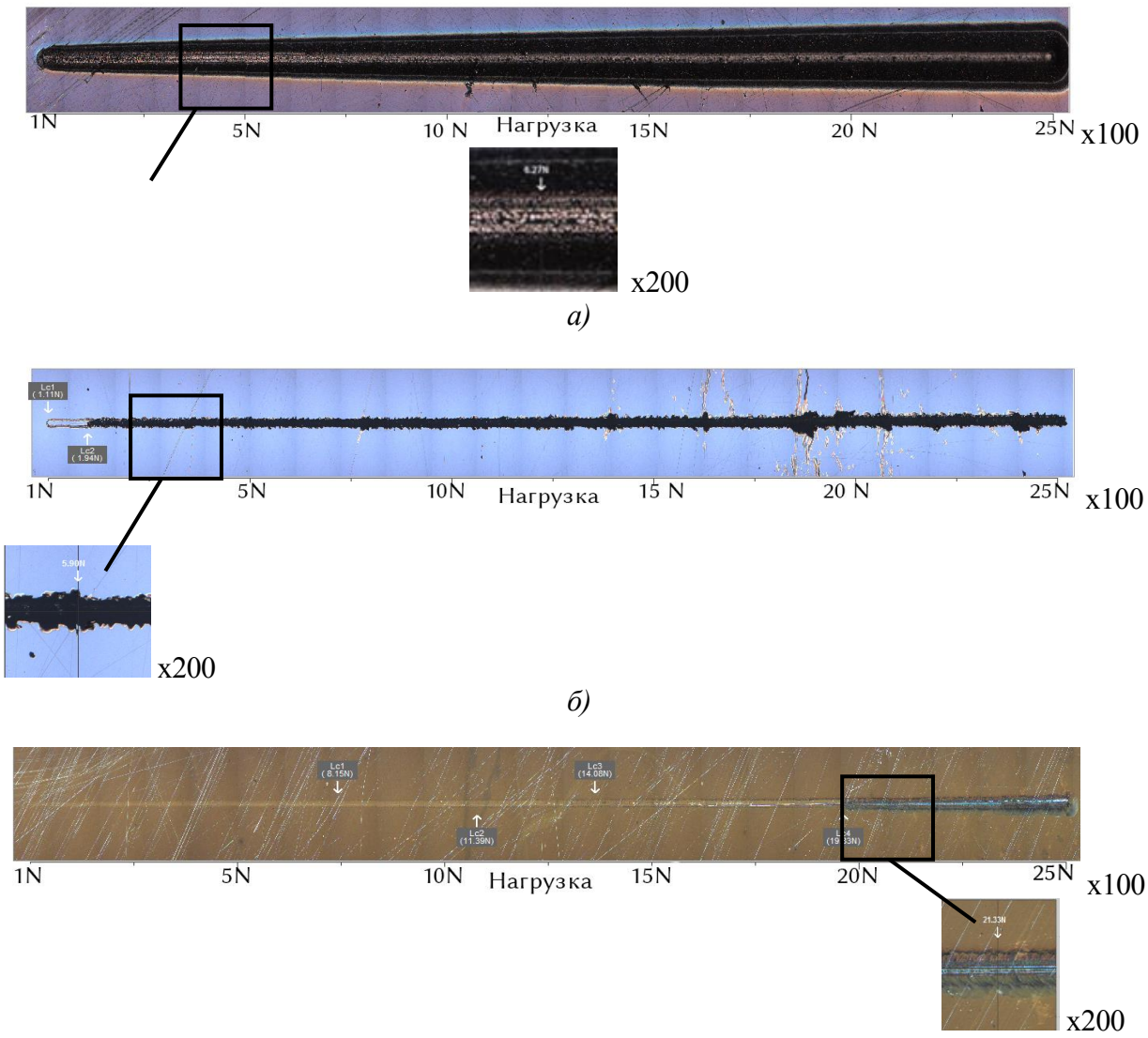
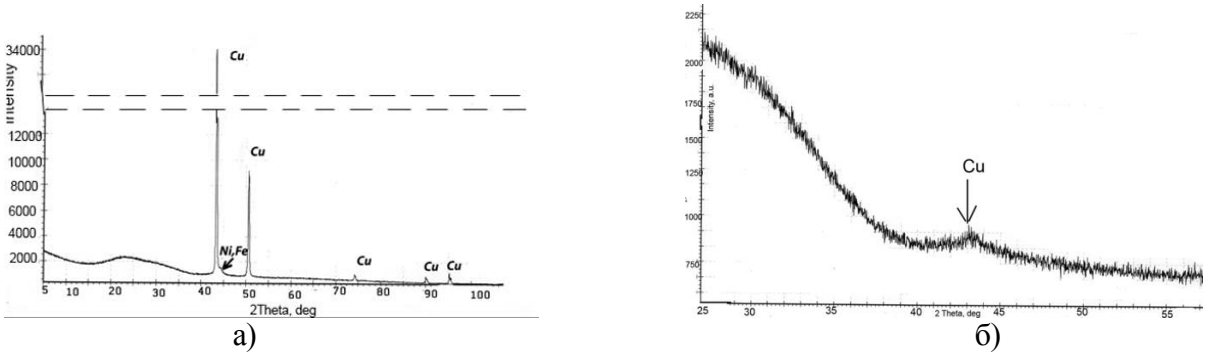


Рис.2. Фрагменты царапин на покрытиях после испытаний:
а - покрытие 100Cu/300Ni80Fe20 на поликарбонате; *б* – покрытие 100Cu/300Ni80Fe20 на стекле; *в* – покрытие $45ZrO_2/5Ni/45ZrO_2/22Cu/2Ni/45ZrO_2$ на стекле



а) б)

Рис.3. Фрагменты рентгенограмм покрытий, полученных электронно-лучевым методом:
а - 100Cu/300Ni80Fe20; б - $45ZrO_2/5Ni/45ZrO_2/22Cu/2Ni/45ZrO_2$

Установлено, что структура двухслойного покрытия100Cu/300Ni80Fe20, нанесенного на подложку из поликарбоната на подложке из поликарбоната, представляет собой поликристаллическую пленку меди со средним размером зерна 9,5 нм Параметр элементарной ячейки a = 0,36129 нм соответствует литературным данным, что

свидетельствует от том, что данная фаза не является твёрдым раствором. А слой пермаллоя Ni-Fe на рентгенограмме практически не проявляется. Возможно небольшой пик интенсивности при $2\theta \approx 45^{\circ}$ связан с наличием этой фазы.

В покрытии $45ZrO_2/5Ni/45ZrO_2/22Cu/2Ni/45ZrO_2$ на стеклянной подложке из кристаллических компонентов обнаружена только медь. Остальные составляющие покрытия имеют аморфную структуру. Параметр элементарной ячейки, также соответствует литературным данным. Средний размер кристаллитов меди меди $D \approx 0{,}470$ нм [7].

Таким образом, покрытия состава 100Cu/300Ni80Fe20 рекомендуется для экранирования корпусов электронных объектов, а состава $45ZrO_2/5Ni/45ZrO_2/22Cu/2Ni/45ZrO_2$ – для дисплев. Данные разработки могут быть использованы в качестве экранов защиты от ЭМИ в радиочастотном диапазоне длин волн, как аналоги применяемых в мировой практике дорогих и/или сложных в изготовлении и/или токсичных экранов (алюминиевые и медные пластины, сетки, стеклопакеты, заполненные специальными растворами, углеродосодержащие конструкции, ITO-покрытия и др.).

Литература

1. Шапиро Д.Н. Основы теории электромагнитного экранирования. Л., 1975.
2. Алексеев, А.Г. Физические основы технологии Stealth / А.Г. Алексеев, Е.А. Штагер, С.В. Козырев. С.-П.: ВВМ, 2007. – 270 с.
3. Крылов В.А., Юрченкова Т.В. Защита от электромагнитных излучений. М., 1972.
4. Волочко А.Т. Защитные нанокристаллические экранирующие покрытия / Перспективные материалы и технологии: монография под ред., В.В. Клубовича. – Витебск, 2015. –глава 3, С. 49−68.
5. Волочко А.Т. Оптически прозрачные экраны электромагнитного излучения // Доклады БГУИР. – 2015. – № 3. – С. 53–57.
6. Scratch Tester JLST022. Install Manual and User Guide. 2-nd Edition 11/2014 | J&L Tech Co.,Ltd.
7. Справочник «Технология тонких пленок»: в 2 т. / редкол.: Л. Майссел, Р. Глэнг. – М.: Сов. Радио.

УДК 004.056.53

Воробьев Владимир Иванович
Главный научный сотрудник
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук (СПИИРАН)
Санкт-Петербург, Россия
Петров Михаил Юрьевич
Ведущий программист
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук (СПИИРАН)
Санкт-Петербург, Россия

ЗАЩИТА ДАННЫХ В КОНВЕРГЕНТНЫХ ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

Существующий опыт переноса информационных услуг в виртуальную инфраструктуру показывает свою эффективность и надежность, а также возможность более широкой виртуализации технологий. Так, перспективным направлением развития является включение виртуальных ресурсов в единую среду управления. Одна из целей интеграции облачной платформы заключается в создании системы, управляющей существующими АИС виртуальных информационных сервисов, создании шаблонов виртуальных машин и унификации программной платформы[1].

Проведены эксперименты по расширению функциональности кластера СПИИРАН, включая развитие индивидуальных решений, использование гипервизоров других типов, в том числе XEN, Xen Cloud Platform, KVM, что позволит снизить совокупную стоимость владения и обеспечить надежную систему управления виртуальными ресурсами. В данном случае обеспечивается горизонтальное масштабирование вычислительных ресурсов и виртуализация гетерогенных программных систем на одной аппаратной платформе. Уникальной характеристикой является поддержка вычислителей разного типа, включая стандартные микропроцессоры, потоковые вычислители на базе графических ускорителей и специализированные решения[2].

Конвергенция достигается за счет переноса – частичного или полного – функциональности оборудования с аппаратного уровня на программный, исполняемый на серверах общего назначения. Поэтому класс такого виртуализованного оборудования уже в меньшей степени определяется «железом», что позволяет на программном уровне обеспечить приложению именно те характеристики аппаратной платформы, какие ему необходимы в конкретный момент времени.

В основу конвергентной инфраструктуры на физическом слое, положена вычислительная ткань (fabric computing), эта технология в контексте повторяет Grid-системы, в частности, на многих проприетарных схемах присутствует Server Fabric. Показана роль больших данных в конвергентных структурах. Данные растут непредсказуемо, а точнее – предсказуемо растут неструктурированные данные. Одно из решений в работе с большими данными – переход к единому транспорту для передачи различных типов трафика, и конвергенция на уровне ядра сети, которая реализуется на базе высокопроизводительных коммутаторов Ethernet.

Конвергенция возможна, как разных видов систем одного функционального назначения, например сервер хранилища данных(СХД) или серверов различной архитектуры, так и систем разного назначения – серверов, СХД и активного сетевого оборудования, в единый вид информационно-коммуникационного оборудования, выполненного на принципах модульности и открытой архитектуры. При реализации единого вида конвергентной структуры важным шагом является проверка основного свойства открытых систем –интероперабельности. Выполнение данного свойства позволяет сократить сроки обработки, передачи и получения больших объемов данных; увеличить надежность работы системы в целом; снизить риск потери и искажения данных или появления ошибок при их передаче; облегчить процесс установки средств защиты от внешних угроз.

Разработан алгоритм и методика для оценки степени интероперабельности любых групп систем, основанный на методах интервальной и экспертной взвешенной оценки и включающий этапы: выделение набора свойств, необходимых для оценки степени интероперабельности рассматриваемой группы систем, и их подробная детализация; выделение интервалов значений для каждой детализированной единицы каждого свойства; присвоение каждой детализированной единице одного из четырех рангов согласно интервалам значений, в которых они находятся; расчет средних рангов свойств, характеризующих степень интероперабельности для каждой рассматриваемой системы; расчет совокупного взвешенного ранга системы.

Предлагается онтологическая модель оценки уязвимости, состоящая из базы данных уязвимостей, семантического обработчика естественного языка и базы данных кодов атак. База данных уязвимостей содержит семантическую коллекцию уязвимостей и связана с базой сценариев атак, построено отображение между подмножествами базы уязвимостей и подмножествами базы сценариев атак. Используется также база кодов атак – компиляция кодов атак из известных баз типа Metasploit. База данных атак используется для запуска атак на приложения с целью тестирования соответствующей уязвимости. Модель упрощает сканирование и оценку уязвимостей приложения[3].

Разработан способ построения гибкой модели обнаружения аномалий информационных потоков, включающий: клиент-серверную архитектуру распределённой системы, её компонентов и схемы взаимодействия между ними, сетевой сенсор, перехватывающий и сортирующий информационный поток, анализатор, получающий данные о потоке от сенсора и рассчитывающий метрики – показатели интенсивности аномалии, база данных, разбитая на 3 части: описательная часть хранит информацию о потоках, типах используемых протоколов, измеряемых признаках, метриках, критериях аномалий; статистические данные по измеряемым величинам содержат таблицы с данными по протоколам, метрикам, событиям по угрозам; административная часть хранит информацию о пользователях системы[4,5].

На кластере Санкт-Петербургского института информатики и автоматизации РАН продолжены расчёты геофизических объектов институтом океанологии РАН. В

частности, для моделирования гидрофизических течений использовался подход, основанный на решении уравнений Рейнольдса. В пространственной области дискретизация осуществляется методом Петрова-Галеркина. Аппроксимация производных имеет второй порядок точности. Система линейных алгебраических уравнений решается методом сопряженных градиентов. Расчеты выполнялись с помощью кода FlowFES-MPI. Также совместно с Северо-Западным УГМС проводятся оперативные расчеты по нескольким моделям (WRF - гидродинамические модели прогноза погоды).

Повышение функциональности кластера СПИИРАН будет способствовать эффективности расчетов многомасштабных приложений в рамках сотрудничества с академическими и другими организациями.

Литература

1. Александров В.В., Воробьёв В.И., Кулешов С.В., Левоневский Д.К., Марков В.С., Фаткиева Р.Р., Юсупов Р.М. Глава 5. Формирование и развитие информационной инфраструктуры инновационного развития Санкт-Петербурга. В монографии: Перспективные направления развития науки в Петербурге. / Отв. ред. Ж.И. Алфёров, О.В. Белый, Г.В. Двас, Е.А. Иванова. - СПб.: Изд-во ИП Пермяков С.А., 2015. - 543 с.

2. Воробьев В. И., Петров М. Ю., Шкиртиль В. И. Моделирование многомасштабных процессов на кластерных структурах. Информационно-измерительные и управляющие системы №9, т. 11, 2013, С.43-49 (ВАК, РИНЦ 0.206)

3. Воробьев В.И., Евневич Е. Л. Онтологический подход к оценке уязвимости облачных вычислений. I международная конференция «Проблемы информационной безопасности», пгт. Гурзуф, 26-28 февраля 2015 г. С. 105-107.

4. Левоневский Д.К., Фаткиева Р.Р. Исследование комбинированных атак класса «отказ в обслуживании». Труды СПИИРАН. 2014. № 1 (32). С. 199-209.

5. Воробьев В.И., Рыжков С.Р., Фаткиева Р.Р. Защита периметра в облачных вычислениях. Третий национальный суперкомпьютерный форум (НСКФ-2014) Переславль-Залесский 25-27 ноября 2014 г. http://www.nscf.ru/materialy-foruma/

6. Шишкин В.М., Савков С.В. Использование знаний экспертов в условиях структурной и метрической неопределенности в риск-анализе // Труды конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14». Научное издание в 4-х томах. – М.: Физматлит, 2014.

УДК 658.5: 001.895

Герасимова Светлана Васильевна
д.э.н., профессор
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ В ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

Информация в ресурсной базе современных предприятий давно играет одну из значимых ролей при организации бизнес-процессов. Нынешние реалии вынуждают менеджеров постоянно осуществлять мониторинг окружающей среды, в частности отслеживать факторы внешней и внутренней среды предприятия, а также изучать контактные аудитории. Как известно, там, где генерируются ресурсы предприятий, всегда присутствует угроза их потери. Сама собой формулируется проблема обеспечения безопасности информации или профилактика и нейтрализация информационных рисков.

Единого научного подхода к определению сущности информационного риска не существует. Но привлекает внимание в большей мере мысль относительно толкования информационного риска с использованием системного подхода, т.е., речь идет об ущербе предприятия, нанесенном не только в результате нарушения безопасности информации, как это встречается в большинстве подходов, но и в результате снижения других важных показателей качества информации [1].

Современные научные исследования указывают на то, что в большей степени интерес у конкурентов предприятия вызывает внутренняя информация, связанная с

технологическими инновациями. Именно эта сфера системы безопасности предприятия нуждается в эффективных управленческих решениях, направленных на сохранение и повышение уровня конкурентоспособности этого предприятия и обеспечение необходимой конфиденциальности.

Решение менеджера должно базироваться на предварительном анализе источников информации об инновациях. Носителями такой информации, как правило, являются внутренние структурные подразделения предприятия, имеющее отношение к инновационной деятельности, в частности, научно-исследовательские и производственные подразделения, венчурные группы, маркетинговые службы и др.

Как показывает статистика, в период 1993-1995 г.г. научно-исследовательские и производственные подразделения имели самый высокий рейтинг в составе источников информации для технологических инноваций, в период с 2003 г. по 2005 г. наиболее рейтинговыми источниками выступили маркетинговые службы и организационные структуры в составе группы, в которую входит организация, последние были характерны и для периода 2011-2013 г.г. [2, с. 45].

С точки зрения теории, управление какими-либо рисками предприятия представляет собою совокупность мер, направленных на идентификацию, анализ и оценку, мониторинг, нейтрализацию и профилактику рисков.

К основным методам анализа рисков относят методы качественного и количественного анализа. Качественный анализ предполагает идентификацию рисков, выявление источников и причин их возникновения, определение потенциальных сфер и зон риска, выгод и негативных последствий риска. Количественный анализ связан с вычислением допустимого уровня риска. Разновидностями количественного анализа рисков являются: анализ безубыточности, финансового состояния, чувствительности, сценариев развития; экспертный, комбинированный, имитационный методы; вероятностный метод и метод аналогий и др.

Некоторые авторы общеизвестные методики классифицируют по типу используемой в них процедуры принятия решения: одноэтапные и многоэтапные методики. Одноэтапным методикам (электронные таблицы типа "Risk Matrix") присуща оценка риска, выполняемая с помощью одноразовой решающей процедуры, многоэтапным (NIST, CRAMM) - с предварительным оцениванием ключевых параметров [3, с. 70].

Выбор методики анализа и оценки информационных рисков, связанных с разглашением информации об инновационных разработках предприятия, при таком их изобилии и многогранности сложен. Анализ убытков, которые предприятие может понести в этой связи, возможен при использовании экономико-статистических и расчетно-аналитических подходов.

Например, Е.А. Козлова предлагает вычисление риска информационной безопасности с помощью следующей формулы [4]:

$$Riskvalue = R(A, T, V) = R(L(T, V), F(Ca, Va)), \quad (1)$$

где R — функция вычисления риска,
A — активы,
T — угрозы,
V — уязвимости,
Ca — стоимость активов, принесенная инцидентом,
Va — степень уязвимости,
L — возможность угрозы привести к инцидентам с помощью уязвимостей,
F — потери, вызванные событиями безопасности.

Как отмечалось выше, применение методов количественного анализа позволяет определить допустимый уровень риска. В частности, допустимым уровнем риска считают риск, который в данной ситуации при существующих общественных ценностях приемлем. Меж тем, встречается более конкретное мнение по поводу уровня рисков предприятий малого и среднего бизнеса, не превышающее 5 %. Данная позиция аргументирована тем, что годовой объем выручки таких предприятий может составлять

до 400 млн. руб., следовательно, убыток (в случае реализации угроз) более 5 % недопустим [5, с. 86].

Таким образом, результаты анализа и оценки информационных рисков в инновационной деятельности предприятий служат основой для разработки соответствующих управленческих стратегий, в частности ИТ-стратегий, а также для разработки рекомендаций по подбору персонала и работы с ним.

Литература:

1. Завгородний В.И. Системный подход к управлению информационными рисками / В.И. Завгородний // Научное, экспертно-аналитическое и информационное обеспечение стратегического проектирования приоритетных национальных проектов и программ. Ч. 2. Сб. науч. тр. ИНИОН РАН. Редкол.: Пивоваров Ю.С. (отв. Ред.) и др. - М.: ИНИОН РАН, 2009, с. 377-383.
2. Индикаторы инновационной деятельности: 2015 : статистический сборник / Н.В. Городникова, Л.М. Гохберг, К.А. Дитковский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2015. – 320 с.
3. Карпов Э.А. Оценка информационных рисков по методике CRAMM / Э.А. Карпов, И.Н. Косарева, А.Г. Кобзева // Вісник НТУ «ХПІ». - 2013. - № 52 (1025). – С. 69-72.
4. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации [Текст] / Е. А. Козлова // Молодой ученый. — 2013. — № 5. — С. 154-161.
5. Плетнев П.В. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П.В. Плетнев, В.М. Белов // Доклады Томского государственного университета систем управления и радиоэлектроники: журнал. - № 1 (25), часть 2, июнь 2012 г. – С. 83-86.

УДК: 378.011.3-051:347.778-049.65

Гордиенко Т.П.
д.п.н., профессор
Смирнова О. Ю.
ассистент
кафедра бизнес-информатики и математического моделирования
Институт экономики и управления
ФГАОУ «КФУ им. В.И.Вернадского»
Республика Крым, Россия

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ПРЕПОДАВАТЕЛЯ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Современные требования к преподавателю в условиях социально-экономических реформ предусматривают владение им соответствующими педагогическими технологиями и методиками, информационно-комуникационными технологиями, применение их в работе, а также наличие у него умений распространять собственный опыт.

Являясь участником инновационного процесса в высшем учебном заведении, преподаватель разрабатывает программы по учебным дисциплинам, составляет учебно-методические пособия, создает электронный имидж образовательного учреждения.

И в этом рабочем процессе преподаватель является не просто автором продукта творческой деятельности, а ее собственником или пользователем интеллектуальной собственности другого автора.

Интеллектуальная собственность (условный собирательный термин) включает права, относящиеся к литературным, художественным и научным произведениям, научным открытиям, изобретениям и т.д.

Несколько упрощая, можно сказать, что к интеллектуальной собственности относится информация, которая может быть представлена на материальном носителе и распространена в неограниченном количестве копий по всему миру. Собственностью являются не эти копии, а отражаемая в них информация.

Недостаточное знание основ авторского права, а также собственных прав на результаты интеллектуальной деятельности и средства индивидуализации приводят к неправомерному заимствованию полезной информации при составлении дидактических материалов, нарушению авторских прав преподавателя.

Вместе с тем преподавателям необходимо знать, что права на результаты интеллектуальной собственности и средства индивидуализации включают в себя:

- интеллектуальные права,
- авторские и смежные с ними права,
- патентные права,
- право на селекционные достижения,
- право на топологию интегральных схем,
- право на секрет производства (ноу-хау),
- права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий,
- право использования результатов интеллектуальной деятельности в составе единой технологии.

Каждая группа таких прав имеет собственные правовые механизмы регулирования. Защита прав интеллектуальной собственности, регистрация интеллектуальной собственности в Российской федерации осуществляется по нескольким направлениям:

- регистрация авторских прав на произведение,
- патентование изобретения,
- регистрация товарного знака,
- международная регистрация прав.

В Российской Федерации результаты творческой деятельности (интеллектуальная собственность) регулируются нормами национального законодательства, а также нормами международных договоров.

К международным договорам, в которых участвует Российская Федерация, относятся следующие:

- Парижская конвенция, Бернская конвенция, Стокгольмская конвенция, соглашение о взаимном признании авторских свидетельств и иных охранных документов на изобретения, заключено в Гаване 18 декабря 1976 г.;
- Страсбургское соглашение о Международной патентной классификации от 24 марта 1971 г., соглашение стран СНГ от 24 сентября 1993 года "О сотрудничестве в области охраны авторского права и смежных прав";
- соглашение о сотрудничестве по пресечению правонарушений в области интеллектуальной собственности от 6 марта 1998 г.

Патентные услуги агентства интеллектуальной собственности (патентное бюро): регистрация товарных знаков, регистрация торговых марок, регистрация этикеток, регистрация упаковок; патентование промышленных образцов;

- патентование изобретений, патентование полезных моделей; регистрация программ для ЭВМ и баз данных; подготовка и регистрация лицензионных, авторских и иных договоров; договоры интеллектуальной собственности;

- проведение патентный исследований, патентный поиск; защита объектов авторского права; помощь в разрешении конфликтов в сфере интеллектуальной собственности; представительство и ведение дел по защите прав в Роспатенте, в антимонопольных органах и судебных инстанциях; международная защита интеллектуальной собственности; управление интеллектуальной собственностью; экспертиза проектов, патентная экспертиза; коммерциализация, трансфер технологий, интеллектуальной собственности; учет (аудит) объектов интеллектуальной собственности; оценка объектов интеллектуальной собственности; консультации по вопросам защиты интеллектуальной собственности; разработка патентной стратегии предприятия и многое другое.

При Федеральной службе по интеллектуальной собственности, патентам и товарным знакам создан консультативный совет.

Основная его цель - поиск эффективных путей защиты собственности, выработка предложений по совершенствованию законодательства, создание среды для здоровой конкуренции и благоприятного инвестиционного климата.

УДК 004.62

Железнов Дмитрий Валерианович
д.т.н., доцент
Курунов Александр Владимирович
к.т.н.
Ткаченко Сергей Павлович
к.т.н., доцент
Самарский государственный университет путей сообщения

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ САМАРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ПУТЕЙ СООБЩЕНИЯ КАК ЭЛЕМЕНТ ОБЩЕЙ КОНЦЕПЦИИ БЕЗОПАСНОСТИ ВУЗА

При эксплуатации компьютерных систем возможна потеря информации на жестких магнитных дисках (ЖМД) и съемных носителях. Это может произойти из-за физического повреждения диска, записи неверной информации, случайного уничтожения файлов, действия вредоносных программ. Для того чтобы уменьшить риски до приемлемого уровня и предотвратить потери данных в таких ситуациях, следует создавать периодически обновляемые резервные копии. В случае, если резервное копирование возложить на конечного пользователя, то выполнение протокола безопасности подвергнется угрозе из-за человеческого фактора, например недисциплинированности. Известны случаи, когда и системные администраторы считают нормальным производить не ежедневное резервирование критичных данных, а осуществлять его через достаточно большой промежуток времени. Такая ситуация неприемлема не только с точки зрения общей концепции безопасности ВУЗа, но и, например, в бухгалтерских расчетах, идущих нарастающим итогом.

Бурное развитие компьютерной техники и внедрение ее для автоматизации деятельности ВУЗа вызвало лавинообразный рост объема оперативной информации и количества резервных копий. Информационная система Самарского государственного университета путей сообщения (СамГУПС) базируется на программных продуктах 1С — 1С:Унииверситет, 1С:Бухгалтерия, 1С:Зарплата и кадры, 1С:ITIL, 1С:Документооборот, 1С:Управление автотранспортом. В университете для поддержания этой инфраструктуры используется 13 физических серверов IBM x3250 и один сервер IBM BladeCenter E, на котором реализован отказоустойчивый кластер из 12 виртуальных серверов. Общий объём оперативной информации составляет около 5 Тб, а объем резервных копий – 9,5 Тб. При определении рационального плана архивирования такого объёма данных, ставилась задача добиться оптимизации расходов времени и средств на хранение резервных копий при условии надлежащего поддержания надёжности и восстановления информации.

Анализ аппаратных средств для резервного копирования, приведенный в табл. 1, показал, что съёмные диски и кассеты не обеспечивают приемлемой скорости резервирования, особенно для систем 1С (предполагающих онлайн-копирование), а твердотельные накопители — приемлемой цены хранения.

Таблица 1.

Характеристика накопителей для резервного копирования

Название	Емкость 1 носителя, Гб	Скорость работы от скорости ЖМД	Цена за Гб, US$
DVD Диски	4,7-9	0,1	0,03
Жесткие диски	До 6 000	1	0,1
Магнитная лента LTO	1 600	0,1	0,01
Твердотельные носители	До 2 000	10	0,4

Для хранения данных выбрана система на основе ЖМД дисков IBM DS3400.

Размещение системы хранения данных (СХД), как правило, в одном помещении с серверами, делает её уязвимой, как в случае чрезвычайных ситуаций (пожар, затопление, и т.д.), так и при несанкционированном доступе (НСД) в режимное помещение. В СамГУПС, с целью реагирования в случае нештатных ситуаций, разработан план по восстановлению информации из резервных копий, часть которого отображена в табл. 2

Таблица 2.

План резервирования

Роль сервера	Объем данных, Гб	Номер сер-верной	Номер сервер-ной с СХД	Периодичность резервирования	Проверка состояния резервных копий
Критически важные сервисы					
1С Бухгалтерия	14	2	3	ежедневно	ежедневно
Сервер баз данных 1С	4	2	3	ежедневно	еженедельно
Интенет шлюз, DHCP сервер	40	1	3	ежедневно	еженедельно
Узел почтового кластера	500	1	3	ежедневно	еженедельно
Узел почтового кластера	500	3	1	ежедневно	еженедельно
Сайт СамГУПС	500	1	3	ежедневно	еженедельно
Средней важности сервисы					
АРМ «Нагрузка ВУЗа»	1	2	3	ежедневно	ежемесячно
Сервер библиотеки	300	1	3	еженедельно	еженедельно
Некритичные сервисы					
FTP-сервер	500	1	3	еженедельно	ежемесячно
Не требующие периодического резервирования сервисы					
Сервер приложений 1С	30	2	3	после установки	ежегодно
Контроллер домена	40	1	3	после установки	ежегодно
Сервер свидетель для Exchange	40	3	1	после установки	ежегодно
Сервер видеоконференций	6	3	1	после установки	ежегодно
Сервер Bacula	6	3	1	при измерении	ежегодно

План аварийного восстановления информации предусматривает архивное хранение данных в резервной СХД, расположенной географически удаленно от основного серверного помещения. По этому плану все сервера разделены по категориям. Для критически важных сервисов, куда входят, в первую очередь, сервера баз данных 1С на базе PostgreSQL, применяется система непрерывного архивирования и восстановления на момент времени (Point-in-Time Recovery (PITR). Комбинируется резервное копирование на уровне файловой системы с резервным копированием файлов журнала опережающей записи (WAL), что дает возможность восстановить базы данных к их состоянию на любое время с момента выполнения резервной копии.

Для сервисов средней важности применяется еженедельное полное копирование, для некритичных сервисов — ежемесячное полное копирование. Для серверов, с редко изменяемой информацией после установки или изменения конфигурации сервера производится снятие образа диска.

Для снижения затрат на одну единицу хранения информации нами применена система резервного копирования с открытым кодом Bacula. Выполненная по клиент-серверной архитектуре, эта система выполняет функции резервирования и восстановления Linux, Windows серверов и клиентских машин. Имеется возможность применять различные варианты резервирования– такие как полный, дифференциальный или инкрементальный, а так же ротацию резервных файлов. Таким образом создана система резервирования информации, позволяющая обеспечить приемлемый уровень безопасности хранения данных при относительно низких затратах на реализацию.

УДК 004

Журавленко Николай Иванович
кандидат юридических наук, доцент
Тутова Ольга Васильевна
кандидат педагогических наук
кафедра гуманитарных и социально-экономических дисциплин
Крымского филиала Краснодарского университета МВД России

СПОСОБЫ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Совершенствование компьютерных технологий все более приближает нас к тому времени, когда значительная доля информационных ресурсов будет содержаться в электронном виде. Сегодня практически нет ни одной сферы человеческой деятельности, в которой не использовались бы компьютеры, позволяющие создавать, накапливать, хранить, обрабатывать и передавать огромные объемы информации. Создание электронно-вычислительной техники большой производительности, ее широкое внедрение в экономическую, социальную и управленческую деятельность привели к повышению значимости информации и информационных ресурсов. В то же время динамичное внедрение новейших электронных систем и коммуникационных средств в различные сферы деятельности современного общества не только привело к развитию положительных тенденций в науке и технике, искусстве и образовании, но и выявило ряд факторов негативного характера.

Продолжающаяся криминализация общества сопровождается развитием негативных тенденций, связанных со злоупотреблениями возможностями компьютерной техники. Многочисленные известные факты совершения новых видов преступлений, связанных с использованием средств компьютерной техники и информационных технологий, показывают, что сама компьютерная техника может быть как предметом преступного посягательства, так и инструментом совершения преступлений различными способами[1].

Под способом совершения преступления в криминалистике понимают объективно и субъективно обусловленную систему поведения субъекта, оставляющего различного рода характерные следы в период, предшествующий преступному деянию, в момент совершения преступления и после его совершения. Эти следы позволяют с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, собственно, определить наиболее оптимальные пути раскрытия преступления.

Иными словами, способ совершения преступления слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке своих действий, представляющих в информационном плане своеобразную модель преступления.

Способ совершения преступления всегда является результатом совокупного действия значительного числа факторов. Чем больше они будут проявляться в

[1] Панфилова Е.И., Попов А.С. Компьютерные преступления. СПб., 1998. С. 5

действиях, тем больше следов будет оставлять преступник, и тем большей информацией будут располагать следователь и оперативный работник для выдвижения следственных и оперативно-розыскных версий.

Противоправные деяния подобного рода можно условно разбить на несколько групп:

1) преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых;

2) преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ;

3) преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве орудия или средства совершения корыстного преступления, а умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо введения в компьютерную систему ложной информации.

Критерием разграничения между предметом, орудием и средством совершения преступлений в сфере компьютерной информации является характер использования различных предметов в процессе совершения преступления. Поэтому следует различать компьютерную информацию, на которую осуществляется неправомерное воздействие (такая информация является предметом преступления), и компьютерную информацию, которая является орудием совершения преступления, посредством которой осуществляется неправомерное воздействие на предмет преступления (например, на денежные средства).

В качестве предмета преступления в сфере компьютерной информации могут выступать различные виды защищаемой информации: объекты авторского права; государственная, банковская и коммерческая тайна; персональные данные и сведения, составляющие тайну частной жизни, и др. В качестве орудия совершения преступления в сфере компьютерной информации могут выступать команды, вводимые с клавиатуры или с помощью звуковых сигналов, различного рода «вирусные» и «троянские» программы, а также иная вредоносная информация, способная осуществить неправомерное воздействие на предмет преступления[2].

Рассматривая в качестве орудия киберпреступлений информационно-телекоммуникационные сети, специалисты говорят о понятии так называемой дорожки электронно-цифровых следов, которая может служить средством для обнаружения признаков преступления и установления обстоятельств содеянного. Один из ведущих отечественных специалистов-правоведов в области борьбы с компьютерными преступлениями В.Б. Вехов определяет это понятие как систему образования следов в компьютерной сети, состоящую из нескольких последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование операторов связи от компьютера преступника до компьютера потерпевшего [3].

Все способы совершения компьютерных преступлений в отечественной криминалистической науке классифицируются по пяти основным группам, которые, в основе своей, соответствуют градации, приведенной в ст.ст. 2-8 Концепции Совета Европы «О киберпреступности». Основным классифицирующим признаком в данном случае является метод осуществления подозреваемым тех или иных преступных деяний, направленных на получение доступа к средствам электронно-вычислительной техники.

---

[2] Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Н. Новгород, 2000. С. 12.

[3] Соколов А. В. Защита информации в распределённых корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – С. 78-85.

В соответствии с этим выделяются следующие основные группы методов совершения компьютерных преступлений:

1) непосредственное изъятие средств электронно-вычислительной техники;
2) перехват информации;
3) несанкционированный доступ к ЭВТ;
4) манипуляции с данными и управляющими командами;
5) комбинированные методы.

Рассмотрим каждую из этих групп более подробно. К первой группе относятся традиционные способы совершения преступлений корыстной или иной направленности, в ходе которых действия преступника направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимаются средства ЭВТ. С уголовно-правовой точки зрения подобные преступления квалифицируются по соответствующим статьям Уголовного кодекса РФ, например, ст.ст. 276 (Шпионаж), 158 (Кража), 162 (Разбой), 163 (Вымогательство) и др. Характерной чертой данной группы способов совершения компьютерных преступлений является то обстоятельство, что в данном случае средства ЭВТ выступают только в качестве предмета преступного посягательства, а в качестве орудий совершения преступления (если таковые применяются) используются иные инструменты, технические устройства и приспособления, не являющиеся средствами электронно-вычислительной техники. Наиболее типичным примером такого вида преступлений является кража персональных компьютеров, содержащих в своей постоянной памяти какие-либо сведения, представляющие интерес для злоумышленника. Сюда же можно отнести и различные способы преступных деяний, связанных с противоправным завладением различными физическими носителями информации: магнитными и оптическими дисками, электронными кредитными картами и т. п. Такие способы совершения преступлений достаточно основательно изучены отечественной криминалистической наукой и в дальнейших комментариях не нуждаются.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях подозреваемых, направленных на получение машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата. Следует отметить, что в этой и последующих группах способов совершения компьютерных преступлений средства ЭВТ могут выступать и в качестве предмета, и в качестве орудия совершения преступного посягательства.

Существует несколько разновидностей рассматриваемого способа совершения преступлений.

А. Непосредственный (активный) перехват. Он осуществляется посредством прямого подключения к оборудованию компьютера или информационно-телекоммуникационной сети, например, к линии принтера или телефонному проводу канала связи, используемых для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В связи с этим различают:

1) форсированный перехват, представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;
2) перехват символов – выделение из текста, набираемого пользователем на клавиатуре терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;
3) перехват сообщений – несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Нередко подобное подключение осуществляется с помощью бытовых средств и оборудования: телефона, отрезка провода, телефонного кабеля, компьютерного многопроводного шлейфа, зажимов типа «крокодил», специальных щупов-игл от контрольно-измерительной аппаратуры, набора радиомонтажных инструментов, кассетного портативного магнитофона, принтера, модема, либо персонального

компьютера типа «ноутбук». После подключения к каналу связи вся информация записывается на физический носитель или переводится в визуально воспринимаемую форму посредством бытовой или специальной электронной аппаратуры.

Могут также применяться и специализированные устройства, например так называемые «кейлогеры» - закамуфлированные под переходники или шнуры-удлинители устройства, подключаемые к линии связи между системным блоком компьютера и клавиатурой. Они записывают на внутреннюю память каждое нажатие клавиш на клавиатуре, что позволяет злоумышленнику, периодически получая к ним доступ, читать все набранные тексты, узнавать коды доступа к различным информационным и коммуникационным ресурсам пользователя (его электронной почте, страничкам в социальных сетях, зашифрованным файлам и архивам и т. д.).

Б. Электромагнитный (пассивный) перехват. Существуют перехватывающие устройства, которые не требуют непосредственного подключения к системе. Соответствующие сведения могут быть получены не только по каналам связи, но и в помещениях, где расположены средства коммуникации, и даже на значительном удалении от них. В связи с этим электромагнитное излучение, возникающее при функционировании средств компьютерной техники, включая и средства коммуникации, можно зафиксировать на физическом носителе без прямого контакта с информационно-телекоммуникационной сетью.

Излучаемые волны с учетом их определенного ослабления, как показывают результаты экспериментов, можно принимать на расстоянии до 1 километра от места передачи. Как только эти сигналы приняты специальной аппаратурой и переданы на компьютер подозреваемого, появляется возможность получить изображение, идентичное тому, которое возникает на мониторе обладателя информации. Для этого достаточно лишь настроиться на соответствующую индивидуальную частоту.

Каждый компьютер можно идентифицировать по его конкретным параметрам: рабочей частоте, интенсивности электромагнитного излучения и ряду других технических параметров. Поэтому для осуществления преступных целей иногда достаточно смонтировать приемную антенну по типу волнового канала, имеющую более острую, несимметричную диаграмму направленности, после чего разработать (или использовать готовую) программу расшифровки «перехваченных» данных.

Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 г. в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании PTT Вим-Ван-Эк шокировал специалистов тем, что с помощью разработанного им устройства из своего автомобиля, находящегося на улице, «снял» данные с экрана дисплея персонального компьютера, установленного на 8 этаже здания, расположенного в 100 м от указанного места.

При совершении компьютерных преступлений указанным способом подозреваемыми, как правило, незаконно используются методы оперативно-розыскной деятельности и специальная техника (например, соответствующие сканирующие устройства).

В. Аудиовизуальный перехват. Данный способ совершения преступления заключается в действиях подозреваемого, направленных на получение информации путем использования различной видео- и аудиотехники. Этот способ предусматривает эмпирическую и электронную формы фиксации получаемых сведений.

В первом случае перехват информации производится визуальным путем с использованием различных видеооптических приборов, например, подзорной трубы, бинокля, охотничьего прибора ночного видения, оптического прицела и т. п. Наблюдение за объектом осуществляется с определенного расстояния, и полученная информация фиксируется на материальном носителе лишь после завершения перехвата. Орудие преступления находится непосредственно в руках подозреваемого. Получить и зафиксировать аудиоинформацию в этой ситуации достаточно сложно.

Во втором случае процесс получения аудио- и видеоинформации осуществляется с использованием специальной техники. Обычно применяются записывающие или передающие устройства, которые скрытно размещаются на объекте наблюдения: спецвидеомагнитофоны с длительной записью, оборудование для скрытой аудио- и видеосъемки, видеокамеры и т. п.

Г. «Уборка мусора». Этот способ совершения преступления заключается в неправомочном использовании подозреваемым технических отходов информационного процесса, оставленных обладателем сведений после завершения работы с компьютерной техникой. Он реализуется в двух формах: материальной и электронной.

В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, емкостей для технологических отходов и сбору находящихся в них физических носителей информации.

Электронный вариант совершения преступления предполагает просмотр, а иногда и последующее исследование данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования ЭВТ. Например, последние записанные данные не всегда стираются из оперативной памяти компьютерной системы после завершения ее работы.

В некоторых случаях могут осуществляться действия по восстановлению и последующему анализу данных, содержавшихся в файлах, которые были стерты со сменных носителей информации. Достигается это за счет использования в качестве орудия преступления определенных программных средств специального назначения, относящихся к инструментальным программам.

К третьей группе способов совершения компьютерных преступлений относятся деяния, направленные на получение несанкционированного доступа непосредственно к средствам компьютерной техники. Можно выделить следующие способы совершения такого вида преступлений.

А. «За дураком». Типичный прием физического проникновения хорошо известен специалистам в области ОРД. Он заключается в следующем: имея при себе элементы маскировки, подозреваемый заходит в помещение, где находится предмет посягательства, следуя за кем-либо из сотрудников организации, имеющих в него санкционированный доступ. Данный вариант получения незаконного подхода к ЭВМ рассчитан на низкую степень бдительности работающего персонала и службы охраны объекта.

Б. «За хвост». Этот способ перехвата информации заключается в следующем. Подозреваемый с использованием средств компьютерной связи подключается к линии связи законного пользователя и терпеливо дожидается сигнала, означающего конец работы, после чего переключает его «на себя», а затем, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе. Этот способ технологически можно сравнить с работой двух и более незаблокированных телефонных аппаратов, соединенных параллельно и работающих на одном абонентном номере: когда телефон «А» находится в активном режиме, на другом телефоне «В» поднимается трубка; после того, как разговор по телефону «А» закончен и трубка положена, – разговор продолжается с телефона «В».

В. «Компьютерный абордаж». Данный способ совершения компьютерного преступления осуществляется подозреваемым путем случайного подбора абонентного номера компьютерной системы «жертвы» с использованием, например, обычного телефонного аппарата. Иногда для этих целей используется изготовленная кустарным либо промышленным способом программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы с использованием быстродействия современных компьютерных устройств перебрать все возможные варианты комбинаций букв, цифр и специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае «угадывания» пароля произвести автоматическое соединение с соответствующим абонентом.

Следует обратить внимание на наличие множества программ-«взломщиков», именуемых на профессиональном языке HACK TOOLS (инструменты взлома). Однако они становятся малоэффективными в компьютерных системах, обладающих программой-«сторожем» компьютерных портов. Поэтому в последнее время хакерами активно используется метод «интеллектуального перебора», основанный на подборе пароля, исходя из заранее определенных тематических групп его предполагаемого содержания. В этом случае с помощью программы-«взломщика» анализируются персональные данные автора пароля и другие, непосредственно связанные с ним сведения. Как показывают многочисленные эксперименты, вручную с использованием метода «интеллектуального перебора» вскрывается около 42% от общего числа паролей. По существу «компьютерный абордаж» является подготовительной стадией компьютерного преступления.

Г. «Неспешный выбор». Подозреваемый осуществляет несанкционированный доступ к компьютерной системе путем обнаружения слабых мест в ее защите. Обычно такой способ используется преступником в отношении тех обладателей информационных систем, которые не уделяют должного внимания регламенту их проверки.

Д. «Брешь». В отличие от «неспешного выбора» данный способ предполагает поиск подозреваемым участков в защите компьютерной системы, имеющих ошибку или неудачную логику программного построения. Выявленные подобным образом «бреши» могут использоваться хакером многократно, пока они не будут обнаружены самим обладателем компьютерной информации. Появление подобного способа обусловлено тем, что программисты нередко допускают ошибки при разработке компьютерных программ, которые не всегда удается обнаружить в процессе отладки программного продукта.

Е. «Маскарад». Подозреваемый проникает в компьютерную систему под видом законного пользователя. Системы защиты средств компьютерной техники, не обладающие функциями идентификации пользователей по биометрическим персональным данным (отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются в этом случае бессильными. Самый простой путь к проникновению в такие системы – получение кодов и других идентифицирующих шифров законных пользователей. Это можно сделать в результате приобретения списка пользователей со всей необходимой информацией путем подкупа, шантажа или иных противоправных деяний в отношении лиц, имеющих доступ к той или иной информационной системе.

К четвертой группе способов совершения компьютерных преступлений относятся действия подозреваемых, связанные с использованием методов манипулирования данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений экономической безопасности и противодействия коррупции органов внутренних дел. Рассмотрим способы, наиболее широко практикуемые в криминальной практике.

А. Подмена данных – наиболее простой и потому довольно распространенный способ совершения преступлений. Действия подозреваемых, осуществляемые, как правило, при вводе-выводе информации, направлены на изменение существующих данных либо ввод новых данных. С помощью данного способа можно приписать тому или иному банковскому счету «чужую» историю, то есть модифицировать данные в автоматизированной системе банковских операций. Следствием этого становится появление в ней денежных сумм, которые реально на данный счет не зачислялись.

Б. «Рекламные закладки или Adware» – это достаточно серый тип программ. Он может быть как хорошим, с точки зрения безопасности, так и вредоносным. Примером хорошего варианта является установка бесплатных программ, которые так же устанавливают необходимый код для последующего просмотра рекламы. В этом случае вы бесплатно получаете функциональность, но за это просматриваете рекламу, от которой разработчик программы получает доход. Однако, среди Adware существует и

немало вредоносных программ, которые без ведома владельца отправляют личную информацию рекламодателям или же встраивают рекламные блоки в другие программы, например, в браузеры.

В. «Пугающие или вымогающие вредоносные программы» – эти программы, в основном, полагаются на психологическое воздействие (страх, угрозы и прочее) и требуют перевести средства или нажать на ссылку, перейдя по которой начнется установка трояна или другой вредоносной программы. Технически, не редко такие программы используют только разрешенные и безопасные функции системы, из-за чего средства безопасности просто не обращают на них внимания. А если и используют сомнительные функции, то на очень примитивном уровне.

Г. «Скрытые индикаторы» – применяются для сбора информации о владельце компьютера. В отличие от программ-шпионов, чаще всего они используют разрешенные методы. Например, вставка на страницу или в электронное письмо прозрачной картинки размером 1 на 1 пиксель. Смысл в данном случае заключается в том, что при загрузке данной картинки с внешнего сервера, на нем записывается не только время и дата запроса, но так же и вся информация, которую он только сможет получить, например IP-адрес компьютера и версию браузера. С одной стороны, такой тип программ сложно назвать вредоносным. С другой стороны, без ведома владельца на стороннем сервере собираются личные данные, пусть и часто публичные.

Д. «Троянский конь». Данный способ заключается в тайном введении в программное обеспечение законных обладателей информации специально созданных компьютерных программ. Разместившись в чужих информационно-вычислительных системах (обычно под видом известных сервисных программ), они начинают выполнять новые, незапланированные законными обладателями информационных ресурсов команды, с сохранением прежней работоспособности ЭВМ.

Особый вид составляют так называемые «банковские трояны». Они позволяют устанавливать полный контроль над зараженным компьютером. Троян собирает и передает данные об используемой системе интернет-банкинга, состоянии счета и информацию о проводимых платежах. Он же позволяет злоумышленникам формировать и проводить мошеннические платежные поручения[4].

С помощью данного способа подозреваемые нередко перечисляют на заранее подготовленные счета определенные денежные суммы с различных банковских операций. Возможен также вариант увеличения злоумышленником избыточных сумм на своих собственных счетах в результате автоматического перерасчета рублевых остатков при переходе к новым коммерческим курсам валют.

Программа «троянского коня» обнаруживается с большими сложностями, как правило, высококвалифицированными экспертами-программистами. Для ее поиска необходимы значительные временные затраты.

«Троянский конь» имеет следующие разновидности:

1. «Троянская матрешка». Особенность этого способа заключается в том, что программные модули-фрагменты, определяющие состав «троянского коня», по окончании возложенной на них миссии самоуничтожаются. Найти их затем практически невозможно.

2. «Троянский червь». Его специфика, напротив, помимо основных нелегитимных функций программы «троянского коня» предполагает и действия, направленные на ее автоматическое самовоспроизведение. «Программы-черви» копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети), используя для этого алгоритм действия компьютерных вирусов, о которых речь пойдет ниже.

3. «Салями». Такой способ совершения преступления стал возможным благодаря использованию компьютерных технологий в бухгалтерских операциях. Он основан на

[4] См.: Как обезопасить свои финансы: интервью начальника Управления экономической безопасности и противодействия коррупции ГУ МВД России по г. Москве Ю. Васильева. С. 18.

методике проведения операций перевода на подставные счета незначительных сумм – результата округлений, которые на профессиональном бухгалтерском языке называются «салями».

С позиций логики правонарушителей, это один из простейших и «безопасных» способов совершения преступлений. Он используется обычно при хищении денежных средств в ходе тех бухгалтерских операций, в которых с каждой операции отчисляются дробные (меньше, чем одна минимальная денежная единица) суммы денег, поскольку в этих случаях всегда осуществляется округление сумм до установленных целых значений. Подозреваемые рассчитывают на то, что при каждой проверке потерпевший теряет незначительную сумму, которая практически не фиксируется документально.

4. «Логическая бомба». Иногда из тактических соображений хищение удобнее всего совершать при стечении каких-либо обстоятельств, которые в перспективе обязательно должны наступить. Подозреваемыми используется способ совершения преступления, основанный на тайном внесении в программу потерпевшей стороны набора команд, которые должны сработать (или срабатывать каждый раз) при наступлении определенных обстоятельств. Далее включается алгоритм программы «троянского коня». Разновидностью «логической бомбы» является «временная бомба», которая срабатывает по достижении определенного момента времени.

5. Компьютерные вирусы. Как уже отмечалось, с программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов, искажение и стирание данных и информации, переполнение машинной памяти, создание помех в работе ЭВМ и др. Такие программы обычно составляются на языке программирования Assembler и не выдают при своей работе никаких аудиовизуальных отображений в компьютерной системе.

Этот способ совершения компьютерного преступления является ничем иным, как логической модернизацией способа «троянский конь», выполняющего алгоритм типа «сотри все данные этой программы, перейди в следующую и сделай то же самое». Его использование имеет весьма широкое распространение.

Для удобства анализа специалисты дифференцируют существующие вредоносные программы по определенным самостоятельным группам:

1) загрузочные (системные) вирусы (поражающие загрузочные секторы машинной памяти);

2) файловые вирусы (поражающие исполняемые файлы, в том числе COM, EXE, SYS, BAT-файлы и некоторые другие);

3) комбинированные вирусы.

Заражение загрузочными вирусами происходит при загрузке компьютера с носителя машинной информации, содержащего вирус, который может попасть на него даже в том случае, когда пользователь только вставил его в приемное устройство (дисковод) зараженного компьютера и, например, прочитал оглавление.

Файловые вирусы заражают компьютер в том случае, если пользователь запустил на своей ЭВМ программу, содержащую вирус. В этом случае возможно заражение и других исполняемых файлов. Многие вирусы выявляются не сразу: первое время компьютер «вынашивает инфекцию», вирус как бы наблюдает за всей обрабатываемой в системе потерпевшего информацией и может перемещаться вместе с ней. Начиная действовать, он подает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программное управление. Потерпевший ничего не замечает, поскольку его компьютерная система находится в состоянии «здорового носителя вируса». Через некоторое время происходит нарушение нормального режима функционирования ЭВМ: компьютер отказывается нормально загружаться или не загружается совсем; по неизвестным причинам исчезают из памяти файлы; некоторые программные средства самопроизвольно стираются из памяти; на экране дисплея начинают перемещаться буквы и символы (вирус «листопад», «змейка», «мозаика»);

исчезают системные файлы с определенным расширением (например, com, bat, exe, txt и т. д.); резко на 180 градусов переворачивается изображение; на экране дисплея неожиданно появляется рекламное изображение и т. п.

Следует также отметить, что заражение компьютерным вирусом может применяться как самостоятельно, так и в сочетании с другими преступными деяниями. В последнем случае эта операция, как правило, выполняет роль маскирующего фактора, способствующего сокрытию основного совершаемого преступления. Невиртуальным аналогом подобных действий является, например, поджог складского помещения после похищения материальных ценностей из него[5].

6. «Веб-инжекты». Для хищений денежных средств физических лиц злоумышленники активно используют техники «веб-инжектов». Это новый вид троянских программ, которые не воруют логин и пароль для доступа к счету онлайн-банкинга, а используют более хитроумную схему, заставляя пользователей самостоятельно перечислять деньги на чужой счет. Для мошенников крайне важно совершить перевод денег с банковского счета жертвы на подставной счет и впоследствии обналичить похищенные средства в максимально короткие сроки.

Существуют специальные сервисы, которые позволяют задавать в заголовке SMS-сообщения, приходящего на мобильный телефон жертвы, номера отправителя и получателя. Поэтому, когда приходит сообщение, в поле «От кого» может указываться любой номер или текст, заданный отправителем через подобный сервис. В самом сообщении может содержаться предложение отправить SMS на короткий номер или перейти по ссылке. В случае такого перехода на мобильный телефон жертвы загружается программное обеспечение, способное не только снимать деньги со счета мобильного телефона, но и распространять рекламу, ссылки на поддельные сайты, а также перехватывать одноразовые пароли для «Клиент-банка»[6].

В. Моделирование. При совершении компьютерных преступлений все более распространенным становится использование подозреваемым компьютерного моделирования, имитирующего поведение устройства или системы. Моделируются, как правило, те процессы, в которые злоумышленники намерены вмешаться, а также разрабатываемые способы совершения преступления. Например, с целью ухода от налогообложения используется так называемая «черная» или «двойная» бухгалтерия, основанная на существовании двух одновременно работающих программ автоматизированного бухгалтерского учета с взаимоперетекающими контрольными данными. Одна из них функционирует в легальном режиме, а другая – в нелегальном для проведения незаконных (теневых) бухгалтерских операций.

Существует несколько основных типов компьютерного моделирования, к примеру, создание реверсивной модели, сущность которой заключается в следующем. Создается модель конкретной системы, на которую планируется совершить вторжение. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем подбираются максимально приближенные к действительности желаемые результаты. После этого модель совершения преступления «прогоняется» назад, к исходной точке, и подозреваемому становится понятно, какие манипуляции с входными – выходными данными необходимо совершить, чтобы достичь желаемого результата.

Это далеко не исчерпывающий перечень способов совершения компьютерных преступлений данной группы. Многие их варианты довольно трудно поддаются описанию, поскольку постичь их сущность можно лишь с помощью языка программирования. Нередко они выполняют вспомогательную роль в ходе подготовки и реализации основных рассмотренных способов[7].

---

[5] См.: Мелик Э. Криминалистическая характеристика компьютерных преступлений // URL: http://www.melik.narod.ru/glava_2.html (дата обращения: 03.06.2012).

[6] См.: Как обезопасить свои финансы: интервью начальника Управления экономической безопасности и противодействия коррупции ГУ МВД России по г. Москве Ю. Васильева. С. 18.

[7] Журавленко Н.И., Яковец Е.Н. Правовые основы защиты информации: Учебное пособие. – Уфа: РИЦ БашГУ, 2015. – С. 172-189.

К пятой и последней группе способов совершения компьютерных преступлений относятся комбинированные методы, под которыми понимается использование подозреваемым одновременно двух и более вышеуказанных способов, а также их различных сочетаний.

Раскрытие преступлений, связанных с информационными технологиями достаточно трудоемкий и сложный процесс. Тем не менее, органами внутренних дел уже проведены как организационные, так и практические мероприятия, направленные на совершенствование борьбы с компьютерными преступлениями. В частности, в Следственном комитете при МВД России создан отдел по организации расследования преступлений в сфере компьютерной информации, а в следственных управлениях крупных регионов – специализированные подразделения по расследованию данного вида преступлений. Оперативно-розыскная деятельность по выявлению, пресечению и раскрытию правонарушений в сфере телекоммуникаций и компьютерной информации осуществляется имеющимся в министерстве Управлением по борьбе с преступлениями в сфере высоких технологий и его подразделениями на местах.

В завершение следует отметить, что выявление и исследование новых видов компьютерных преступлений требует еще немалых дополнительных усилий со стороны ученых и практических работников. Тем, кто непосредственно ведет борьбу с преступностью в столь проблемной сфере, следует постоянно углублять свои знания, практические навыки и умения. Специалисты в этой области не должны замыкаться в узком корпоративном кругу. Для расширения профессионального кругозора им необходимо регулярно знакомиться с научными публикациями, участвовать в научно-практических конференциях, обмениваться опытом со специалистами в других областях права, приобретать личный исследовательский опыт.

УДК 32.019.5

Журавленко Николай Иванович
кандидат юридических наук, доцент,
кафедра гуманитарных и социально-экономических дисциплин
Крымского филиала Краснодарского университета МВД России
Шведова Лариса Евгеньевна
кандидат технических наук,
доцент кафедры информационно-полиграфических технологий
Таврической академии (структурное подразделение)
ФГАОУ ВО «КФУ им. В.И. Вернадского»

ПРОБЛЕМЫ БОРЬБЫ С ИНФОРМАЦИОННЫМ ТЕРРОРИЗМОМ

Информационный терроризм за последние два десятка лет превратился в одно из наиболее опасных проявлений высокотехнологического терроризма, а информационные технологии стали его новой базой. Исследователи М. Девост, Б. Хьютон, Н. Поллард определяют информационный терроризм как сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов [1].

Одним из основных направлений ведения информационного терроризма является воздействие на информационные ресурсы и аппаратно-программные средства противника. В качестве примера такой информационной агрессии можно назвать разрабатываемое и осуществляемое США и их союзниками в целях завоевания геополитического господства в мире программно-математическое воздействие на информационный ресурс потенциального противника, в т. ч. и России. Зависимость России от зарубежных разработчиков компьютерной техники и программного обеспечения приводит к появлению в нашей информационной инфраструктуре множества уязвимых мест, обуславливающих возможность вторжения в эту сферу

вероятного противника. Такое вторжение может выражаться в массированных групповых и одиночных программных ударах, специальных операциях и систематических действиях по выявлению наиболее важных объектов информационных ресурсов нашей страны, заблаговременному установлению над ними скрытого контроля с целью последующего выведения их из строя.

Потенциальный противник способен реализовать свое преимущество в применении таких средств информационного воздействия, как программно-компьютерная атака и оружие направленной энергии, получивших общее название «некинетическое оружие» или «кибероружие».

Известно, что разведслужбы США используют современные компьютерные технологии для тотальной слежки за всем миром, нередко оказывая при этом соответствующие услуги американским корпорациям в борьбе с конкурентами. Причем имеются примеры и обратного свойства, подчас стирающие грани между политическим, военным, экономическим шпионажем и своего рода «неототалитаризмом». К примеру, французские спецслужбы опубликовали доклад, где утверждается, что «компьютерный гигант «Майкрософт» сотрудничает со спецслужбами США. Создаваемые компанией программы дают возможность следить за действиями пользователей с помощью специальных «закладок», которые при необходимости могут не только «прочитать» нужную информацию, но и вывести из строя те или иные аппаратно-программные средства. К слову сказать, программы «Майкрософт» установлены на сегодняшний день у 90% компьютерных пользователей»[1].

Ярким примером применения кибероружия являются хакерские, по своей сути, атаки на стратегические объекты вероятного противника. Ранее уже приводились примеры подобных нападений, но в них говорилось о частных лицах, реализующих свои преступные замыслы в сфере компьютерных технологий. Однако когда подобные деяния совершаются представителями спецслужб отдельных государств, то это уже выходит за рамки обычной уголовной преступности и обретает очертания государственного кибертерроризма.

Первым подобным примером считается взрыв сибирского газопровода «Уренгой – Сургут – Челябинск» в 1982 г. Газопровод имел стратегическое значение для СССР, в связи с чем США были крайне заинтересованы в выведении его из строя. В начале 1980-х гг. президент Р. Рейган, по некоторым данным, одобрил план диверсии против экономики Советского Союза. В этой связи нашим специалистам под видом технической поддержки была передана компьютерная программа, содержавшая скрытые дефекты. Впоследствии она и спровоцировала взрыв газопровода.

В конце 1990-х гг. на серверы Пентагона, НАСА и нескольких университетов США была проведена кибератака, получившая название «Лабиринт лунного света». Некоторые специалисты полагают, что инициатором ее проведения явился Китай. В середине нулевых ударам хакеров были подвергнуты НАСА и три американские фирмы, имеющие отношение к оборонной промышленности. Эта операция получила название «Титановый дождь» и также, по мнению специалистов, была организована Китаем.

Наиболее громким скандалом последних лет является кибератака на ядерные объекты Ирана, имевшая место в июне 2010 г. Строительство АЭС в иранском городе Бушере осуществлялось российскими специалистами и далеко выходило за сферу интересов США и их союзников. Для выведения из строя системы управления указанной АЭС, на которую иранцы отказывались допускать международных наблюдателей, было предпринято распространение вируса Stuxnet[2]. «Когда мы начали разбирать эту программу, сразу стало ясно, что она нацелена на внедрение в промышленные объекты, – отмечает А. Гостев, главный антивирусный эксперт «Лаборатории Касперского». – А именно: она изменяет настройки систем, отвечающих за работу высокоскоростных

[1] См.: Большой Брат по имени Эшелон. Известия. 2000. 24 февраля.

[2] Говорят, в названии этой программы зашифровано имя персидской царицы иудейского происхождения, которая сорвала когда-то планы истребления евреев на территории современного Ирана.

моторов и насосов или центрифуг. Попав на обслуживающий компьютер, этот «червь» сначала увеличивает скорость вращения мотора, а потом резко ее сбрасывает. Далее цикл повторяется. Понятно, что рано или поздно это приведет к разрушению устройства… Stuxnet отбросил ядерную программу Ирана на несколько лет назад…». Специалисты полагают, что непосредственными организаторами разработки и применения данной вредоносной программы явились США и Израиль[3].

Недавно выяснилось, что спецслужбы начали прятать шпионское программное обеспечение даже в защищенных от удаления и форматирования зонах жестких дисков, выпускаемых крупнейшими производителями. Это теоретически позволяет внедрившей эти программы спецслужбе незаметно считывать данные с большинства используемых в мире компьютеров.

Новые шпионские программы были обнаружены российской «Лабораторией Касперского»[4]. Разработчик антивирусов утверждает, что выявил инфицированные подобным методом компьютеры в 30 странах. На первом месте в этом списке он назвал Иран, затем Россию, Пакистан, Афганистан, Китай, Мали, Сирию, Йемен и Алжир.

Целью слежки были правительственные и военные учреждения, телекоммуникационные и энергетические компании, банки, атомные исследовательские центры, СМИ и исламские активисты. Хотя инициаторы шпионажа могли технически получить доступ ко множеству компьютеров, на самом деле они выбрали в «жертву» ограниченное количество – тех, кем они непосредственно интересовались.

Фирма прямо не назвала, какая именно страна ответственна за подобный шпионаж, однако уточнила, что эта схема тесно связана с уже упоминавшимся выше вирусом Stuxnet, который был использован для атаки на завод по обогащению урана в Иране.

Таким образом, как справедливо отмечает О.В. Дамаскин, «кое-где информационный терроризм стал элементом государственной политики. В некоторых странах активно ведутся работы над компьютерными программами, являющимися информационным оружием. Причем объектами для такого оружия все чаще становятся отдельные личности, социальные группы, принимающие решения, а не только массы и государственные структуры, как это было не так давно. Иными словами, избирательность этого оружия растет, именно люди, в первую очередь высокопоставленные, являются теперь главной целью в информационных войнах, и их принуждают к выбору необходимых противнику решений. Информационное воздействие на государство, общество, отдельно взятого человека, в конечном счете, оказывается более эффективным и экономичным, чем политическое, экономическое и даже силовое военное»[5].

Особенно обострилась тема информационной безопасности государства в прошлом году. Информационная среда и технологии могут применяться в деструктивных целях, и Россия должна находиться в постоянной готовности к противоборству в информационной среде. Для защиты своих интересов в развернувшейся информационной войне необходимы упреждающие меры законодательного регулирования, и в России ведется активная работа в этом направлении. Например, уже введен принцип обязательной аутентификации при подключении к открытым общественным сетям, принят закон, предписывающий хранить пользовательские персональные данные на серверах, расположенных только на территории России. Интернет-компаниям дан год на то, чтобы перенести данные на российские Центры обработки данных. Это позволит обезопасить пользователей от угрозы утечки их информации или отключения от каких-либо сервисов. Однако, как показали разоблачения Эдварда Сноудена, без импортозамещения в сфере информационных

[3] См.: Писаренко Д. Кибервойны. Одной клавишей компьютера можно уничтожить страну // Аргументы и факты. 2011. № 36. С. 40.

[4] «Касперский» выявил американский шпионский вирус // URL: http://lenta.ru/news/2015/02/17/nsavirus/ (дата обращения 16.02.2015).

[5] Дамаскин О.В. Россия в современном мире: проблемы национальной безопасности: Монография. М., 2007. С. 267.

технологий польза от такого переноса пользовательской информации сводится на нет, так как успех в международной конкуренции на информационном поле определяется прежде всего технологической независимостью государства.

Эксперты обратили внимание на то, что информационная безопасность государства должна быть направлена на противостояние не только внешним угрозам, но и внутренним. Так, по данным МВД России, в 2014 году было зарегистрировано около 11 тыс. преступлений, связанных с мошенничеством в Интернете и информационной среде. Из них 41% – мошенничество и кражи[6].

По данным Group-IB (одной из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий) объем мирового рынка киберпреступности выглядит следующим образом: интернет-мошеничество – 426 млн. долл., кардинг (преступления, связанные с банковскими картами) – 680 млн. долл., распространение спама – 841 млн. долл., внутренние сделки (продажа трафика, анонимизация) – 288 млн. долл., DDOS-атаки – 113 млн. долл.

Представители правоохранительных и контролирующих органов отмечают, что развитие современных компьютерных технологий предоставляет новые возможности для совершения преступлений. «Анонимность, различные сервисы предоставления услуг – все это дает возможность злоумышленникам дискредитировать законопослушный сетевой бизнес», – считает начальник Бюро специальных технических мероприятий МВД России Алексей Мошков. С этим утверждением согласен заместитель руководителя Федерального агентства связи Роман Шередин, который считает, что «… информационная среда и технологии тоже могут применяться в деструктивных целях. И Россия должна находиться в постоянной готовности к противоборству в информационной среде»[7].

В данной ситуации единственным реальным выходом из создавшегося положения является наращивание научно-экономического потенциала России, позволяющего производить отечественные средства информатизации и коммуникации. Кроме того, необходима четкая стратегия обеспечения информационной безопасности на государственном уровне и объединение усилий всех субъектов этой деятельности. Здесь уместно упомянуть опыт США и Китая – в этих странах ликвидированы все централизованные точки в компьютерных системах управления, через которые можно проникнуть в сеть и обезглавить целую страну[8]. Для того, чтобы снизить криминализацию информационного пространства необходимо, чтобы все участники информационного рынка, гражданские институты, органы власти и правоохранительные органы объединили свои усилия в обеспечении информационной безопасности.

Список литературы

1. Томас Т.Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. М., 2002
2. Панфилова Е. И., Попов А. С. Компьютерные преступления. СПб., 1998. С. 5
3. Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Н. Новгород, 2000. С. 12.
4. Соколов А. В. Защита информации в распределённых корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – М.: ДМК Пресс, 2002.
5. Смит Р. Э. Аутентификация: от паролей до открытых ключей. – М.: Изд. дом «Вильямс», 2002.

[6] Россия обновит информационную доктрину из-за угрозы кибервойны. URL: http://q99.it/vj92O5p. Дата обращения - 02.03.2015.

[7] Там же.

[8] См.: Писаренко Д. Указ соч. С. 40.

УДК 004.056.53 (075.8)

Козина Галина Леонидовна
к.ф.-м.н., доцент
Запорожский национальный технический университет
Запорожье, Украина
Канаева Наталья Николаевна
к.ф.-м.н., доцент
Крымский институт бизнеса
Республика Крым, Россия

ФОРМИРОВАНИЯ СЛЕПОЙ ПОДПИСИ НА БАЗЕ НАЦИОНАЛЬНОГО СТАНДАРТА

Среди схем электронной подписи различного назначения отдельное место занимает слепая подпись. Слепая подпись [1-3] лежит в основе криптосистем, в которых решается проблема обеспечения анонимности – системах тайного электронного голосования и системах электронных денег. Слепой называется подпись, сформированная под замаскированным сообщением. В процессе подписания подписант не имеет возможности ознакомиться с содержанием открытого (незамаскированного) сообщения. Слепая цифровая подпись позволяет автору документа доказать его юридическую значимость, не раскрывая своей личности.

В типовой схеме слепой подписи, как правило, принимают участие три стороны - эмитент документа, подписант и валидатор. Эмитент создает документ, который должен подписать подписант. При этом подписант не имеет возможности узнать содержания документа и вида окончательной подписи, для чего эмитент маскирует документ с помощью определенного криптографического преобразования. Подписант подписывает замаскированный документ, а эмитент на основе его подписи формирует окончательную подпись под документом в открытом виде в соответствии со схемой слепой подписи. Валидатор проверяет правильность подписи с помощью открытого ключа подписанта.

В схеме электронного голосования в качестве эмитента может выступать избиратель, подписывающего – участковая избирательная комиссия, валидатора - центральная избирательная комиссия. Избиратель заполняет бюллетень, маскирует его, чтобы сохранить конфиденциальность голоса, и передает на подпись в участковую избирательную комиссию. Комиссия, подтвердив личность избирателя, подписывает его бюллетень, не зная, за кого тот проголосовал. Центральная избирательная комиссия получает бюллетень в открытом виде и проверяет правильность подписи участковой комиссии, не зная при этом личности избирателя, заполнившего этот бюллетень.

В случае слепой цифровой подписи к критериям защищенности схемы подписи необходимо добавить свойство анонимности [4] – невозможность отследить по подписанному документу его автора. Впрочем, в некоторых схемах у подписанта может оказаться возможность нарушить анонимность, поскольку в процессе формирования окончательного вида подписи он обменивается с эмитентом документа дополнительными параметрами, предусмотренными схемой подписи. Если подписант сохранит эти параметры, связав их с конкретным эмитентом, а в дальнейшем сможет получить доступ к документу с собственной подписью в открытом виде, то он сможет попытаться вычислить его автора с помощью сохранившихся параметров. Вычислив маскирующие параметры, которые использовал эмитент, подписант сможет однозначно связать его с документом, что приведет к нарушению анонимности. В схеме электронного голосования это означает, что будет известно, за кого проголосовал конкретный избиратель.

Протоколы слепой подписи обычно реализуются на основе известных алгоритмов электронной цифровой подписи. Надежность стандартов подписи, на базе которых можно построить алгоритм слепого подписания, гарантирует защиту подписи от подделки. Обеспечение анонимности является отдельной задачей, и достигается за счет «правильного выбора» маскирующих параметров. В [5] описан алгоритм построения

слепой подписи на базе немецкого стандарта ECGDSA. Предложенный в [5] механизм выбора маскирующих множителей позволяет формировать слепую подпись с выполнением условия анонимности на базе многих стандартов подписи.

В докладе рассматриваются несколько протоколов слепой цифровой подписи электронных документов, построенных на базе национальных стандартов. Для них доказано обеспечение анонимности пользователей.

В протоколах слепой цифровой подписи используются в качестве математических структур мультипликативная группа простого поля, группа точек эллиптической кривой над конечным полем.

Стандартная схема слепого подписания выглядит следующим образом.

После запроса эмитента электронного документа подписант начинает процесс формирования подписи, высылая эмитенту в закрытом виде разовый секретный параметр. Например, возведя в секретную степень генератор мультипликативной группы простого поля или умножив на секретное число базовую точку аддитивной группы точек эллиптической кривой над конечным полем (в зависимости от выбора математической структуры в схеме).

Эмитент, используя полученный от подписанта параметр, привлекает маскирующие множители к этому параметру и открытому ключу подписанта и формирует с их помощью первое число подписи. Далее эмитент маскирует хеш-образ своего документа, полученное первое число подписи и высылает их подписанту для подписывания его секретным ключом.

В момент подписания подписант не знает настоящего хеш-образа документа и первого числа подписи, т.е. подписывает вслепую. Формула подписи должна соответствовать выбранному стандарту подписи, что гарантирует ее надежность. Сформированную подпись подписант высылает эмитенту, и последний имеет возможность проверить подлинность подписи под замаскированным документом.

Эмитент, получив от подписанта слепую подпись, преобразовывает ее и формирует второе число окончательной подписи. Теперь открытый документ и два числа подписи (реально сформированных эмитентом) могут быть открыто опубликованы и проверены валидатором. При этом эмитент документа останется неизвестным, если по результатам общения с подписантом в дальнейшем будет невозможно его отследить, т.е. выполнено условие анонимности. Свойство анонимности достигается в процессе маскирования параметров таким образом, чтобы условие проверки не позволяло вычислить автора документа.

Протоколы подписи, сформированные на базе стандартов с выполнением условия анонимности, могут функционировать в стандартной инфраструктуре открытых ключей.

Литература:

1. Chaum D. Blind signatures for untraceable payments / D. Chaum // Advances in Cryptology, Crypto '82. – Springer-Verlag. – 1983. – P. 199-203.

2 Ростовцев А.Г. Подпись "вслепую" на эллиптической кривой для электронных денег / А.Г. Ростовцев // Проблемы информационной безопасности. Компьютерные системы. – 2000. - № 1. – С. 40-45.

3. Молдовян Н.А. Новые протоколы слепой подписи / Н.А. Молдовян, П.А. Молдовян // Безопасность информационных технологий. – М.:МИФИ. – 2007. – № 3. – С. 17-21.

4. Нікуліщев Г.І. Анонімність як критерій оцінки захищеності протоколів сліпого електронного цифрового підпису / Нікуліщев Г.І., Козина Г.Л. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – №2.–С.52-59.

5. Козина Г.Л. Протокол слепой цифровой подписи на основе стандарта ECGDSA / Козина Г.Л., Никулищев Г.И., Молдовян Н.А. // Вопросы защиты информации. – 2014. – №1.– С.40-45.

УДК 659.4

Пенькова Инесса Вячеславовна
д.э.н., профессор
кафедра бизнес информатики и математического моделирования
Института экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА ПЕРСОНАЛЬНОГО КОНТЕНТА В СОЦИАЛЬНЫХ СЕТЯХ

В наш век высоких технологий и интернета сложно представить жизнь без глоальной сети. И одной из важных страниц социализации членов общества стали социальные сети. Практически у каждого человека есть аккаунт хотя бы в одной сети из многообразного количества варрантов. Наиболее популярными на территории Европы, России и стран СНГ являются сети: Вконтакте, Фейсбук и Одноклассники.

В ходе исследования рассмотрены основные элементы управления сайтом социальной сети, модель регистрации в социальной сети, проанализированы уязвимости и основные багги, а так же изучена документация по сайту. В ходе работы выдвинуты возможные способы решения проблемы потери личных данных и защиты личного контента пользователя.

Отметим, что законодательно хищение или потеря любого типа информации с сайта запрещено и очень быстро пресекается, но в реальной жизни исполнение этой нормы далеко от идеала. Вследствие отсутствия адекватных мер наказания за совершение противоправных действий, и возникающих сложностей по отслеживанию подобную деятельность (так как количество посетителей сайта в день, например в сети «Одноклассники.Ру» насчитывается более 45 миллионов человек) эти противоправные действия все же совершаются и полностью пресечь их невозможно. То есть, пользователь в первую очередь сам должен следить за контентом и его содержанием.

Во избежание утечки информации о пользователях посетителям запрещается собирать информацию о других пользователях и применять ее личных целях, так же использовать для этого любые автоматические средства сбора информации. Нельзя осуществлять пропаганду или агитацию, возбуждающую расовую или политическую, религиозную или национальную борьбу. Так же запрещено передавать закрытую информацию и информацию ограниченного доступа (к такой информации относят файлы с аудио, видео и фото ресурсами, а так же электронные книги). Нарушение авторских прав может повлечь за собой не только административную, но и уголовную ответственность. Особенно, если брать во внимание ужесточение норм использования аудио и видео файлов в России по состоянию на текущий период.

Нельзя передавать оскорбительные материалы в любом виде. Более того, сейчас действует закон, который состоит в выплате штрафа, в размере 5 000 рублей за оскорбление или неуважительное поведение в сети.

В ходе исследования рассмотрены основополагающие понятия и принципы работы социальной сети Одноклассники.ру. Выявлены основные багги этой системы, ключевые минусы и плюсы, определены наиболее важные проблемы уязвимости социальных сетей и выдвинуты возможные пути их решения.

Можно сделать вывод, что защита персонального контента зависит в первую очередь от самого пользователя. Пользователь должен быть внимателен и предельно осторожен, целесообразно тщательно фильтровать информацию, выкладываемую о себе, на свое страничке, внимательно следить за файлами, которые скидываются в сеть.

УДК 004.7

Пестунова Тамара Михайловна
к.т.н., заведующая кафедрой
«Информационная безопасность»
ФГБОУ ВО «Новосибирский государственный
университет экономики и управления»
Белов Виктор Матвеевич
д.т.н., профессор, СибГУТИ
ФГБОУ ВО «Сибирский государственный
университет телекоммуникаций и информатики»
Новосибирск, Россия

К ВОПРОСУ О МОДЕЛИРОВАНИИ И ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-ПРОЦЕССОВ

Постановка задач ИБ в контексте бизнес-процессов позволяет соотнести аспекты безопасности с результатами бизнес-процессов, а значит, и с целями деятельности организации [1-7]. Бизнес-процессы организаций и предприятий не являются статичными. Их изменчивость обусловлена многими причинами, в частности, слиянием фирм, оптимизацией организационных структур, внедрением автоматизированных технологий и т.п., что требует отражения происходящих изменений в системе обеспечения ИБ. При этом изменения могут касаться всех элементов системы ИБ: от концептуальных документов, инструкций и регламентов до состава и конфигурации программно-технических решений.

В данной работе предлагаются способы оценки рисков ИБ, направленные на обеспечение ИБ организаций в контексте непрерывности бизнес-процессов.

Анализ моделей бизнес-процессов даёт возможность отследить влияние происходящих изменений на многие аспекты ИБ. В частности, в [1, 2] и ряде последующих работ авторами был предложен автоматизированный подход к управлению правами доступа на основе анализа EPC-модели [8]. В [7] представлена обобщённая схема взаимодействия бизнес-процессов и среды в контексте которой рассматривается управление ИБ, опираясь на системы комплексной автоматизации деятельности предприятия. Материалы зарубежных источников [3, 4, 5, 9] также показывают, что анализ бизнес-процессов организации имеет большое значение для определения рисков ИБ, а также для построения системы управления ИБ. В частности, в [10, 11] предлагается метод расширения нотации BPMN [12] для управления рисками ИБ. В [13] автор предлагает улучшенную версию нотации EPC, которую обозначает как «Security - Oriented EPC». Данная версия была получена путем расширения языка EPC и его конструкций с целью сопоставления данных с моделью ISSRM [14] для оценки рисков ИБ.

Ниже рассмотрим ряд важных риск-ориентированных аспектов моделирования бизнес-процессов с целью получения данных для дальнейшей оценки рисков ИБ. Во-первых, это критичность (важность) бизнес-процесса К (БП), где БП- бизнес-процесс. Важность процесса определяется степенью его вклада в достижение стратегических целей организации. Бизнес-процесс, критичность которого высока, и связанные с ним активы должны иметь больший приоритет при обеспечении безопасности, нежели бизнес-процессы с более низкой критичностью (при прочих равных параметрах).

Во-вторых, следует обратить внимание на ценность актива относительно конкретного бизнес-процесса Ц (А, БП), где А-актив, используемый в БП. В организации ценность одного и того же актива (информации, ресурса) может быть различна в контексте разных БП.

В-третьих, реализация всех этапов каждого БП требует определенного времени, а сам БП может носить итеративный характер. Время итерации, предполагаемое или рассчитанное на основе реальной ситуации, - нормативное время прохождения всех этапов БП от первого действия до получения результата, достижения цели БП.

Изменение времени возможно из-за ошибок или злоумышленных преднамеренных действий исполнителя, ненадлежащего состояния ресурсов, нарушения своевременности входа процесса, излишних затрат времени исполнителей на реализацию предусмотренных процессом работ, несогласованности действий исполнителей и т.п. Последствиями для организации в данном случае могут быть: срыв сроков выполнения, неполное достижение целей, задержка процесса, излишняя трата ресурсов (финансовых, материальных, человеческих). При этом для различных БП существует различный уровень критичности изменения времени итерации, т.е. насколько критично для организации в контексте ущерба будет изменение времени достижения цели БП. Если каждую итерацию БП рассматривать как ограниченную во времени совокупность взаимосвязанных работ (например, от поступления очередного заказа до его исполнения), то для оценки допустимых сдвигов окончания каждого этапа БП в пределах итерации можно использовать методы управления проектными рисками, в частности методы сетевого планирования с выделением критических путей и расчётом наиболее поздних моментов начала-окончания этапов относительно момента начала итерации процесса. Ущерб от инцидента, повлекшего нарушение некоторого актива, может зависеть от момента времени этого инцидента относительно начала-окончания БП. В частности, возможны случаи, когда инцидент, связанный, например, с нарушением целостности актива, может привести к большему ущербу, если он происходит ближе к окончанию итерации БП, т.е. ближе к достижению цели. При высокой критичности процесса относительно сдвига сроков завершения итерации может не хватить времени для восстановления нормального режима исполнения процесса, либо это восстановление потребует привлечения значительных дополнительных ресурсов и работы в мобилизационном режиме. В результате ущерб от не соблюдения требований ИБ (У) можно представить в виде параметрической функции У(БП, А, Ит), где БП - бизнес-процесс; А – актив, используемый в БП; Ит - потенциально возможный инцидент в момент времени Т.

В нашей работе для оценки критичности БП использован подход [15], согласно которому первым шагом определения критичности является выявление критических факторов успеха (КФУ), под которыми понимаются наиболее значимые показатели, определяющие достижимость бизнес-целей. При разработке стратегии, организация должна сформулировать свою миссию, после чего произвести ее декомпозицию на стратегические цели и подцели. Из всех целей необходимо выбрать N наиболее важных, которые и называют КФУ. Графически концепция этого подхода представлена на рисунке 1.

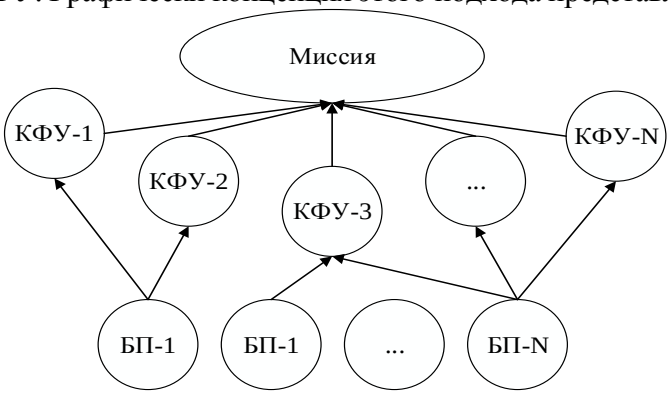


Рис. 1. Критические факторы успеха

Определение критичности (важности) БП является результатом его сопоставления с КФУ. Основная суть сопоставления сводится к тому, что по каждому БП необходимо ответить на вопрос: «Какие КФУ поддерживаются данным БП?». При определении важности БП, помимо сопоставления каждому БП множества КФУ, необходимо совершить обратный проход «сверху вниз», при котором для каждого КФУ определяются поддерживающие его БП.

Таким образом, необходимо построить матрицу сопоставления БП и КФУ, а также определить критичность каждого БП по формуле (1):

$$К_{БП} = \frac{К_{КФУ}}{О_{КФУ}},\ НК_{БП} = 1 - К_{БП}, \quad (1)$$

где $К_{БП}$ – коэффициент критичности БП; $НК_{БП}$ - коэффициент некритичности БП; $К_{КФУ}$ – количество КФУ, относящихся к БП; $О_{КФУ}$ – общее количество КФУ.

На этапе оценки ценности актива (информации, ресурса) необходимо составить перечень активов для каждого БП отдельно, а также определить ценность активов. Важно понимать, что ценность одного и того же актива в контексте различных БП может изменяться. Оценка производится для каждого актива (А-1, А-2, … , А-N) относительно конкретного БП (БП-1, БП-2, … , БП-N) по качественной шкале для каждого аспекта безопасности (конфиденциальность, целостность, доступность). Шкала содержит пять уровней оценки (очень высокий, высокий, средний, низкий, очень низкий), которые определяются уровнем возможного ущерба, полученного организацией при нарушении аспекта безопасности актива в каждом БП. Также рекомендуется применять повышение ценности актива на один или два уровня в зависимости от временного фактора (насколько близко к началу-окончанию итерации БП актив используется).

Учет фактора времени проводят по двум составляющим: коэффициенту критичности сроков (для БП), коэффициенту влияния на срок (для угрозы ИБ). Коэффициент критичности сроков определяют для каждого БП по качественной шкале. Основным критерием оценки является финансовый ущерб или соизмеримые ему иные последствия для организации (репутационные риски, затраты человеческих ресурсов) при изменении времени итерации БП. Коэффициент влияния на срок определяют для каждой угрозы. Следует отметить, что каждая угроза влияет на БП по-разному, в том числе и на временной фактор, в нашем случае на изменение времени итерации БП. Отсюда, для каждой угрозы коэффициент влияния на срок можно представить в виде формулы (2):

$$К_{ВС} = \frac{Т_{\Delta И}}{Т_{И}},\ НК_{ВС} = 1 - К_{ВС}, \quad (2)$$

где $К_{ВС}$ – коэффициент влияния на срок БП; $НК_{ВС}$ – коэффициент независимости от сроков БП; $Т_{И}$ – время выполнения одной итерации БП; $Т_{\Delta И}$ – время изменения выполнения одной итерации БП. Если $Т_{И} = Т_{\Delta И}$ и $К_{ВС} = 1$, то БП можно считать устойчивым к внешним (внутренним) воздействиям, а, следовательно, и защищенным от несанкционированного доступа (НСД). Коэффициент критичности сроков определяют следующим образом:

$$К_{КС} = К_{ВС} * К_{БП}, \quad (3)$$

где $К_{ВС}$ – коэффициент влияния на срок; $К_{БП}$ – коэффициент критичности БП; $К_{КС}$ – коэффициент критичности сроков.

Таким образом, в статье развивается подход [6, 16] к оценке рисков ИБ на основе формальных моделей БП. Проведен анализ существующих методик оценки рисков с выявлением их недостатков в контексте анализа БП. Предложена методика оценки рисков, учитывающая критичность БП, дифференцированность значимости активов относительно БП, а также влияние момента реализации возможных угроз на последствия для БП и связанного с этими последствиями ущерба.

Литература

1. *Пестунова Т.М.* Информационная система управления правами доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Доклады ТУСУРа. – 2010. – № 2 (22), ч. 2. – С. 253–256.
2. *Родионова З.В.* Управление процессом предоставления прав доступа на основе анализа бизнес-процессов / З.В. Родионова, Т. М. Пестунова // Прикладная дискретная математика. – 2008. – № 2. – С. 91–95.

3. *Taubenberger S., Jurjens J.* IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements. InstituteofComputerScience, UniversityofTartu
4. *Rodriguez A., Fernandez-Medina E., Piattini M.* A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE – Transactions on Information and Systems, Volume E90-D Issue 4, March 2007, Pages 745-752
5. *Altuhhova O., Matulevičius R.* Security Risk Management using Business Process Modeling Notations. // Institute of Computer Science, University of Tartu. [Электронный ресурс]. – Режим доступа: http://courses.cs.ut.ee/2015/SSD/spring/Main/Readings
6. *Пестунова Т.М., Родионова З.В., Горинова С.Д.* Анализ аспектов информационной безопасности на основе формальных моделей бизнес-процессов. Доклады ТУСУРа, № 2 (32), июнь 2014 – С. 88–92.
7. *Ефимов Е.Н., Лапицкая Г.М.* Информационная безопасность и бизнес-процессы компании. // Известия ЮФУ. Технич. науки, № 2(149). – Таганрог: ЮФУ, 2013. – С. 45–48
8. Нотация EPC. [электронный ресурс – 17.09.2014] – http://www.businessstudio.ru/wiki/docs/v4/doku.php/ru/csdesign/bpmodeling/epc_notation.
9. *Bradford L., Dumas M.* Getting Started with YAWL. Technical Paper, YAWL Foundation, 2007.
10. *Altuhhova O.* An Extension of Business Process Model and Notation for Security Risk Management. Institute of Computer Science, University of Tartu, 2012. – [Электронныйресурс]. – Режимдоступа: http://courses.cs.ut.ee/MTAT.03.246/2014_spring/uploads/Main/bpmn.pdf.
11. *Altuhhova O.* Developing System Security through Business Process Modelling. Institute of Computer Science, University of Tartu. [Электронныйресурс]. – Режимдоступа: http://courses.cs.ut.ee/MTAT.03.246/2014_spring/uploads/Main/bpmn.pdf.
12. Object Management Group Business Process Model and Notation.–[Электронный ресурс – 15.12.2014]. – http://www.bpmn.org/.
13. *Turan Y.* Extension and Application of Event-driven Process Chain for Information System Security Risk Management. Institute of Computer Science, University of Tartu. – Tartu, 2012. – 114 с.
14. *Chowdhury M.* Modeling Security Risks at the System Design Stage. Master in Security and Mobile Computing, 2011.
15. *Ковалёв С.М.* Выбор бизнес-процессов для оптимизации. // С.М.Ковалёв, В.М.Ковалёв. / "Консультант директора" - 2005, № 5 (232) : [Электронный ресурс]. - Режим доступа:http://www.betec.ru/indexprint.php?id=6&sid=40
16. *Пестунова, Т. М.* Оценка рисков информационной безопасности на основе анализа моделей бизнес-процессов /Т. М. Пестунова, М. С. Кондратьев // Информационное противодействие угрозам терроризма. 2015. - № 24. - С. 44-51.

Сизерон Мари
преподаватель
Университет София-Антиполис
Ницца, Франция

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОТРЕБИТЕЛЕЙ

Ежегодно в мире появляется огромное число новых товаров и услуг, только на полках одного супермаркета их может около 25 тысяч наименований, и каждый год появляются около 8 тысяч. Потребитель, находясь в условиях ограниченного времени на покупку, не имеет возможности подробно знакомиться с каждым новым брендом или его изменившимся ассортиментом и вынужден полагаться на сведения, почерпнутые из рекламы или на возникшие эмоции от упаковки и мнения знакомых. В данной ситуации возникает проблема информационной защиты потребителя, его безопасности.

Практически во всех странах имеются различные правовые механизмы информационной безопасности потребителя. Так, во Франции еще в 1951 году был основан Союз потребителей (некоммерческая организация), издающий журнал «Что выбрать» (UFC-Que Choisir – сайт http://www.quechoisir.org/) и имеющий свой сайт с таким же названием, на котором обсуждаются качество товаров и даются рекомендации по покупкам с целью защиты интересов граждан. Данная организация постоянно закупает и тестирует около 600 товаров, как только новый товар появляется в продаже. Информация о результатах проверки появляется на сайте. Еще до начала экспертизы размещается видео об актуальности товара, его новизне и использовании. Каждый потребитель, зарегистрировавшись на сайте, может участвовать в обсуждении качества товара на форуме.

Во Франции действует принцип свободных цен (Декрет от 1 декабря 1986 года), согласно которому запрещены дискриминационные цены и «лавинная продажа», когда покупателю предоставляется скидка, если он нашел других покупателей на данный товар, это расценивается как мошенничество. Тем не менее, последнее широко практикуется - в Интернет распространяются «группоны» - дешевые билеты на оказание услуги в случае, если наберется определенное число участников группы – потребителей данной услуги. К такому приему часто прибегают индивидуальные предприниматели, составляя тем самым конкуренцию крупным сетям – парикмахерским, спортивным комплексам, танцевальным залам и другим.

Различные союзы и ассоциации потребителей существуют и в других европейских странах, они призваны выражать мнение потребителей, предоставлять дополнительную информацию о товаре, особенно в послепродажный период. Данные организации выполняют, в том числе, посредническую функцию, представляя интересы потребителей в судах в случае нарушения их прав.

С развитием Интернет торговли на сайтах крупных магазинов обязательно размещаются отзывы покупателей о приобретенном товаре, где говорится о скрытых недостатках. Которые невозможно определить только по картинке, например, о тактильных ощущениях, реакции одежды на стирку, дополнительных свойствах (тяжелый-легкий, насыщенность окраски, удобство в использовании и других). Подобные отзывы являются одним из инструментов информационной защиты потребителей.

В ряде стран приняты законы о защите потребителей от рекламы, которая может ввести потребителя в заблуждение, гипнотизировать его для принятия положительного решения о покупке (особенно такое возможно при телевизионной рекламе), вызвать агрессию или другое неадекватное поведение, опасное для здоровья и физической безопасности. также запрещена реклама, содержащая неточности о свойствах товара, сравнивающая рекламируемый товар с аналогичными в пользу последнего, скрывающая происхождение, способы использования товара, использующая страх и суеверия.

Проблема информационной защиты потребителя может быть решена путем взаимодействия государства как законодателя и самих потребителей, их активной позиции.

УДК 002.6; 021

Турдубеков У.Б.
доцент, к.э.н
Налоговая Академия Узбекистана
Худайбердиев Д.С.
директор, ООО «NEW GEN»
Узбекистан

СИНЕРГЕТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО МАРКЕТИНГА НАЦИОНАЛЬНЫХ РЫНКОВ ТРУДА

В условиях глобализации социальных и экономических процессов в мировой экономике оценка национальных рынков труда преследует цель обеспечения желаемой эффективности использования людских ресурсов. «Желаемая эффективность» нами рассматривается глобально, т.е., с точки зрения возможности уравновешивания оценок различных по объему и качеству показателей трудовых процессов в национальных экономиках. Необходимость такого уравновешивания оценок показателей трудовых процессов объясняется тем, что результаты трудовых процессов характеризуются такой системой показателей, которую национальные рынки труда генерируют обособленно, т.е., нет единой методологии формирования социальных и экономических данных по национальным рынкам труда как в статистическом и динамическом аспектах.

Природа отсутствия такой единой методологии кроется, на наш взгляд, в том, что экономические интересы субъектов (людских ресурсов, производственных и непроизводственных структур, обществ, экономик, государств) проявляются элементами ***безопасности.*** Выявление и оценка таких элементов безопасности в цепи «человек – производство – общество – государство – мировая экономика» невозможно без их структурирования в отдельные системы показателей. Именно эти системы показателей являются предметом обеспечения безопасности информационного маркетинга национальных рынков труда.

Функционирование таких систем показателей безопасности в рамках функционирования национальных рынков труда в мировой экономике есть использование национальных ресурсов по глобальному обеспечению безопасности информации о людских ресурсах. Оно выражается не только в удовлетворенности отдельными интересами субъектов в силу данных мер безопасности, но и в эффективности, выражающейся стабильностью безопасности в различных условиях конъюнктурных показателей интересов. Траектория функционирования мировой экономики определяет характер и границы изменения состава показателей безопасности и направления их действия в отдельных национальных экономиках. По сути, речь идет о предельных показателях безопасности, и их следует интерпретировать в контексте синергетики безопасности информационного маркетинга национальных рынков труда.

Синергетика безопасности есть функционирование системы мер безопасности строго в рамках предельных показателей безопасности, понимаемой нами как такое состояние безопасности, что при изменении хотя бы одной меры безопасности происходит изменение состояния (флуктуация) безопасности в целом, оцениваемое как точка бифуркации системы безопасности. Аттракторами в случае с безопасностью информационного маркетинга национальных рынков труда выступают отдельные выгоды, характеризуемые совокупными доходами в рамках национальных рынков труда, к которым стремятся, национальные системы мер безопасности в национальных экономиках. Глобальная цель обеспечения безопасности в данном контексте достижима в том случае, если она будет сформулирована в пределах точек бифуркации и аттракторов безопасности, которые должны описываться унифицированными показателями, при этом их сопоставительные оценки указывают на целесообразность затрат на информационную безопасность в целом в мировой экономике.

УДК 330.46

Шишкин Владимир Михайлович
с.н.с., к.т.н., доцент
Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук

ЦЕНА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ПРИ НЕЛИНЕЙНОМ ИСЧИСЛЕНИИ ЗАТРАТ

Введение.

Понятие критически важного объекта (КВО) в настоящее время широко применяется, оно закреплено официальными документами, определены признаки и перечни таких объектов. Для сферы информационных технологий используются различные частные его варианты, как например, КВИО - критически важные информационные объекты, КВОИИ - критически важные объекты информационной инфраструктуры, встречается и более громоздкий термин - критически важные информационные объекты информационной инфраструктуры (КВИОИИ). Кроме того, защита критических инфраструктур в стратегиях кибербезопасности, принятых в

западных странах (их анализ см. в [1]), является одним из ключевых направлений обеспечения безопасности государств.

Таким образом, в данном контексте понятие критичности несколько изменило смысл по сравнению с традиционным научно-техническим его содержанием, и стало пониматься, следуя англоязычной семантике, преимущественно в смысле важности, исключительной значимости и только, на что мы давно обратили внимание [2]. Далее, учитывая более широкий смысл этого слова, связали критичность с нелинейными переходами и преобразованиями [3], сделав при этом попытку объективной параметризации критических состояний [4]. Такой подход позволил глубже анализировать проявления критичности в приложении к сложным организационно-техническим объектам.

В самом деле, современные объекты реальной, производящей экономики, крупные финансовые структуры, системы государственного, военного управления являются сложными организационно-техническими системами, склонными к нелинейному поведению, и возникновение критических состояний в них не должно считаться исключительным явлением. В структурно сложных объектах незначительный локальный сбой, первичный отказ может сыграть роль малого параметра и привести к непредсказуемому системному эффекту, вплоть до катастрофического.

Сложные организационно-технические системы, должны рассматриваться как нелинейные динамические системы, поведение которых предполагает возможность перехода в критическое состояние в физическом смысле, независимо от их назначения. В то же время такого рода системы часто выполняют интегрирующие, инфраструктурные функции в обеспечении основных видов жизнедеятельности людей, объективно становясь критическими уже в статусном смысле (критически важными). Но и статусное понимание критичности, что заставляет выделять КВО, о чём говорилось выше, неявным образом свидетельствует о нелинейном характере их поведения, по крайней мере, в восприятии меры риска. Рассмотрение критичности в сочетании с нелинейностью в приложении к такого рода объектам имеет различные аспекты, на одном из которых, экономическом, точнее, оценке затрат на обеспечение их безопасности, остановимся ниже.

Неопределённость и противоречия в экономике безопасности.

Определение разумного уровня затрат различных ресурсов на обеспечение безопасности функционирования рассматриваемых систем в условиях присущей им нелинейности, плохой прогнозируемости поведения и неизбежной ограниченности ресурсов является насколько важной настолько же нетривиальной и неоднозначной задачей. С одной стороны, очевидно, неразумны большие затраты при умеренных рисках, но, с другой стороны, может быть, ещё более опрометчивой будет «экономия» при их недооценке. Основная сложность при этом состоит в недостаточной определенности идентификации и оценок рисков, возможность которых ограничена знанием (незнанием) и неизбежным субъективизмом экспертов. Кроме того, не всегда оценки стоимостных показателей в номинальном денежном измерении адекватно отражают реальность.

Затраты на обеспечение безопасности можно при желании наращивать почти неограниченно, либо, наоборот, недооценить потенциальный ущерб. На вопрос, как определить уровень затрат, оптимизирующий суммарные издержки на защиту и остаточный ущерб, как сумму двух разнонаправленных функций, казалось бы давно имеется классический ответ, но практика иногда кардинально ему противоречит, например, в сфере информационной безопасности [5]. К экономике безопасности плохо применимы традиционные подходы, а практика демонстрирует парадоксальное явление одновременного роста как затрат на защиту информационных активов, так и ущерба от нарушений их безопасности. Правда, последнее время рост затрат на обеспечение информационной безопасности замедлился, что, возможно, объясняется «миграцией в облака», но оценить в этом случае затраты на собственно безопасность затруднительно, они становятся неявными, да и ущерб в облаках менее наблюдаем.

Характерна в приложении к рассматриваемой ситуации антиномия, неявно сформулированная в [6]. С одной стороны, утверждается, что «Любой аргумент оценки уровня безопасности должен исходить из того, что твёрдо установлен экономический эквивалент угрозы», но там же в другом месте: «защитные мероприятия … могут быть необходимы и тогда, когда они непосредственно не окупаются экономически». Оба приведённых высказывания, безусловно, справедливы, но как тогда принимать практические решения.

Таким образом, необходим подход, который позволил бы снять формальное противоречие между экономическими ограничениями, с одной стороны, и требованиями безопасности, развития и т.д., с другой, обеспечив между ними рационально обоснованный компромисс. Он становится возможным, если учесть явно нелинейный характер восприятия меры риска в критических приложениях.

Эффекты нелинейного преобразования.

Ранее [3] нами была показана возможность и методика нелинейного преобразования меры риска с использованием функций степенного распределения путем аппроксимации экспоненциального закона распределения, часто используемого в качестве моделей первичных характеристик, связанных со временем. Было признано, что имеются основания считать степенные функции наиболее адекватными как для описания динамических свойств, так и в функциях распределения вероятностей меры риска.

Полученные результаты позволили предложить подход к оценке применения средств защиты информационных активов с нелинейных позиций. Используя представления теории надежности (связав меру риска с временем восстановления) было выполнено нелинейное преобразование временной шкалы, что позволило связать показатели надёжности и безопасности [7]. Далее, полагая, что, «чем дороже время, тем дешевле деньги», естественно было обратить внимание на возможность подобного преобразования для стоимостных характеристик затрат на обеспечение безопасности в условиях критичности.

Коротко покажем выполненные ранее и представленные в [8] преобразования. Определим функции, плотности и интегральную, экспоненциального и степенного законов распределения вероятностей без потери общности, соответственно, в виде (1) и (2):

$$f_{\exp}(t) = \lambda e^{-\lambda t},\ F_{\exp}(t) = 1 - e^{-\lambda t},\ t \geq 0,\ \lambda > 0 \qquad (1)$$

$$f_p(t) = \alpha(t+1)^{-(\alpha+1)},\ F_p(t) = 1 - (t+1)^{-\alpha},\ t \geq 0,\ \alpha > 0 \qquad (2)$$

с математическими ожиданиями

$$m_{\exp}(\lambda) = \frac{1}{\lambda},\ \lambda > 0,\ m_p(\alpha) = \frac{1}{\alpha + 1},\ \alpha > 1. \qquad (3)$$

Положим, что функция (1) представляет распределение некоторых величин в первичной физической шкале, например, временной. Тогда задача отображения первичного распределения в распределение меры риска будет состоять в приближении распределения вида (1) распределением вида (2), учитывая, как показано в [3], что между их параметрами с достаточным качеством можно установить простое соотношение:

$$\alpha = \lambda + 1, \qquad (4)$$

и, далее, в определении параметра степенного распределения в новой шкале при сохранении вида функции, то есть:

$$\alpha_x (t_x + 1)^{-(\alpha_x + 1)} \rightarrow \alpha_z (t_z + 1)^{-(\alpha_z + 1)}, \qquad (5)$$

где α_x и α_z — параметры распределения (2), соответственно, в шкалах t_x и t_z .

Решение этой задачи несложно, однако возникает вопрос, из каких соображений назначать параметр α_z ? Если α_x является либо первичным, физически наблюдаемым, либо определяется из приближения экспоненциального распределения (1) соответственно (4), как $\alpha_x = \lambda + 1$, то для определения α_z необходимо найти то или иное правило, позволяющее его идентифицировать.

Поскольку интегральным показателем риска в некоторой шкале его меры можно считать математическое ожидание соответствующего распределения вероятностей, то довольно естественно, хотя и не обязательно, изменение меры оценивать отношением математических ожиданий исходного и преобразованного распределений. Тогда в нашем случае достаточно задать коэффициент $k_z \geq 1$, выражающий, например, изменение относительной ценности активов, который согласно (3) выразится в следующем виде:

$$k_z = \frac{m_p(\alpha_z)}{m_p(\alpha_x)} = \frac{\alpha_x - 1}{\alpha_z - 1}, \tag{6}$$

откуда не трудно найти искомый параметр:

$$\alpha_z = \frac{\lambda}{k_z} + 1, \tag{7}$$

как функцию от двух параметров: показателя значимости активов k_z и параметра исходного распределения λ, имеющего смысл полезного результата, через которые выразим преобразование исходной шкалы. Для этого используем в качестве аналогии стандартную функцию интенсивности восстановления: $h(t) = f(t)/(1 - F(t))$. Для распределения (2) она выразится в виде $h(t) = \alpha/(t+1)$. Тогда в шкале t_x функция $h(t)$ запишется как $h_x = \alpha_x/(t_x + 1)$, а в шкале t_z как $h_z = \alpha_z/(t_z + 1)$.

Далее введём функцию $H(t) = \int_0^t h(x)dx$, смысл которой можно свести к физическому объему восстановления, и поэтому, очевидно, инвариантную относительно шкал. Следовательно, имеется основание записать равенство $H(t_x) = H(t_z)$, откуда легко определяется искомая зависимость меры риска от исходной меры в номинальном измерении:

$$t_z + 1 = (t_x + 1)^K, \tag{8}$$

где $K = k_z(\lambda + 1)/(\lambda + k_z)$.

Таким образом, оказывается, что $t_z \sim t_x^K$, а показатель K тогда можно считать своего рода релятивистским коэффициентом. Полученное преобразование может представлять самостоятельный интерес для различных приложений, здесь же мы сделаем попытку интерпретировать его в стоимостных категориях, используя указанную выше связь между «временем» и «деньгами» в критических условиях. Отметим, что «время» следует понимать условно, так как вместо него может быть другой параметр (ресурс).

Представим полные издержки в условиях предотвращения или преодоления критических состояний (на обеспечение безопасности, рискованные вложения, технологические скачки и т.п.), как функцию C от качества результата, в традиционном виде суммы монотонных функций, возрастающей - целевых затрат c_0 и убывающей - остаточного ущерба c_r.

Первую из них в наших терминах для простоты выразим в достаточно общем и гибком виде: $c_0 = a\lambda^b, a > 0, b > 0$, как функцию от параметра распределений (1) или (2) в исходной шкале, связанных выражением (4), а вторую – естественно приравнять

математическому ожиданию (3) степенной функции, но уже в преобразованной шкале, и согласно (3) и (7) она запишется как $c_r = k_z / \lambda$. Таким образом функция полных издержек C сводится к виду, где в качестве переменных используются два показателя: $k_z \geq 1$, показатель значимости объекта, выражающий, например, изменение его относительной ценности, и $\lambda > 0$, имеющий смысл полезного результата, например, как аналог интенсивности восстановления.

Тогда функция C, в «линейном» варианте C_L, и для «нелинейной» шкалы стоимости естественно преобразованной соответственно зависимости (8) - C_N, при сохранении вида для c_r выразится следующим образом:

$$C_L = a\lambda^b + k_z / \lambda, \tag{9}$$

$$C_N = (a\lambda^b)^{K^{-1}} + k_z / \lambda. \tag{10}$$

Не приводя здесь вполне обычный анализ введённых функций, оценим качественные закономерности их поведения, хорошо заметные на графиках (рис. 1), построенных при умеренных значениях коэффициентов a и b.

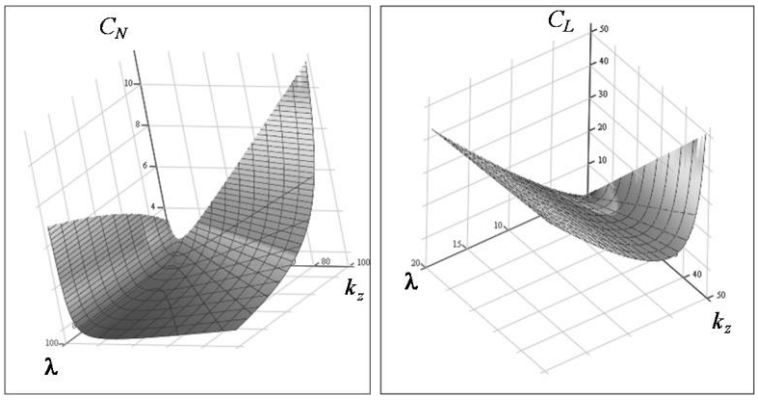


Рис. 1. Сравнительный вид функции полных издержек.

На графике функции C_L видно, что, как ей и положено, она демонстрирует наличие оптимума. Но этот оптимум очень слабо зависит от k_z, и, кроме того, располагается в области малых значений λ, то есть оптимальность затрат при такой постановке задачи никак не определяется значимостью объекта, так как всюду $(C_L)'_{k_z} > 0$, и существенно ограничивает результативность. Но будет ли разумным такое «оптимальное» поведение при больших значениях k_z, то есть когда объект в том или ином смысле критически значим? Этот вопрос, по сути, равносилен следующему, а правильно ли тогда исчислять затраты в номинальном измерении?

График функции C_N радикально отличается от первого. На нём можно обнаружить оптимум, но, во-первых, он слабо выражен, а главное – определяется не λ, так как всюду $(C_N)'_\lambda < 0$, а k_z, при этом для больших k_z и малых λ и, наоборот, малых k_z и больших λ издержки в нелинейном исчислении резко возрастают, т.е. в зависимости от значимости объекта излишняя забота, например, о безопасности может быть столь же экономически неразумна, как и бездействие.

Если ввести в рассмотрение функции эффективности затрат в простейшем выражении соотношения «результат-цена», то тогда, соответственно, $E_L = \lambda / C_L$ и $E_N = \lambda / C_N$. На рис. 2 показаны полученные зависимости.

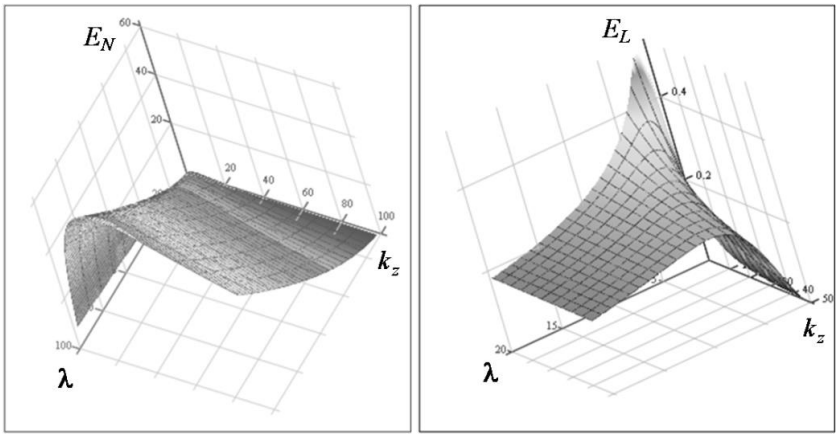


Рис. 2. Сравнительный вид функции эффективности затрат.

На них можно увидеть в целом те же закономерности, которые обнаружились при сопоставлении предыдущих графиков, например, в поведении с точностью до знака частных производных: $(E_L)'_{k_z} < 0$ и $(E_N)'_{\lambda} > 0$. Важно отметить при этом, что, как легко показать, оптимальные значения затрат и их эффективности в принятом смысле не совпадают.

Заключение

Выполненный формальный анализ, как это ни странно, неплохо согласуются с практической деятельностью. Например, руководители далеко не всегда охотно вкладывают средства в информационную безопасность, и, возможно, они, действуя интуитивно, тем более, будучи ограничены в ресурсах, правы? С другой стороны, нельзя исключать чрезвычайные ситуации, когда наиболее экономически эффективной может оказаться политика, следующая принципу «за ценой не постоим». Наглядное подтверждение тому можно видеть на обеих диаграммах, когда при достаточно высокой значимости (критичности) k_z объекта защиты формальный оптимум не достижим, но и суммарные издержки, и эффективность монотонно улучшаются по мере роста интенсивности противодействия λ.

Полученные результаты могут найти применение при прогнозе, планировании, оценке затрат на обеспечение безопасности критически важных, в том числе, инфраструктурных объектов.

Литература

1. Юсупов Р.М., Шишкин В.М. Информационная безопасность и кибербезопасность: семантический конфликт или сосуществование // Информатизация и связь. - № 6 – 2013. С. 8-13.
2. Шишкин В.М., Гололобова О.В. О понятии «критичность» в информационной безопасности // Материалы конференции «Региональная информатика – 2004» (СПб, 22-24 июня 2004 г.) – СПб.: 2004.
3. Шишкин В.М. Степенное распределение и управление рисками критических систем // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук. - 2007. - Т. 31. - М.: КомКнига, 2007. - С. 39-59.
4. Шишкин В. М. «Слабая» критичность в степенных моделях распределения меры риска // Труды СПИИРАН. Вып. 7. — СПб.: Наука, 2008. — С. 119-135.
5. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь, № 1, 2010. - С. 27-35.
6. Фесечко А.И. Оптимизация защитных мероприятий по безопасности жизнедеятельности людей. Надёжность и качество-2011: труды Международного симпозиума: в 2 т./ под ред. Н.К.Юркова. – Пенза: Изд-во ПГУ, 2011. – 2 т. – С.30-31.
7. Шишкин В.М. Показатели надёжности и безопасности: возможности нелинейного перехода. Надёжность и качество -2011: труды Международного симпозиума: в 2 т./ под ред. Н.К.Юркова. – Пенза: Изд-во ПГУ, 2011. – 1 т. – С.100-102.
8. Шишкин В.М. Эффективность, оптимальность и устойчивые пропорции затрат на безопасность при нелинейности меры риска // Надежность и качество - 2012: Труды Международного симпозиума: в 2 т. / под ред. Н.К.Юркова. – Пенза: Изд-во ПГУ, 2012. – 1 т. - С. 123-127.

УДК 371.314

Яблочников Сергей Леонтьевич
доктор пед. наук, проф.
Академия ФСИН
Яблочникова Ирина Остаповна
кандидат пед. наук
докторант Института высшего образования НАПУ

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Сфера образования в целом и высшего профессионального образования в частности, это классические сложные информационные системы (ИС), основная цель функционирования которых – передача знаний, как некоторой совокупности обобщенной информации, от одного поколения человечества к другому. Поэтому решение проблем информационной безопасности, характерных для систем приема, передачи, хранения и обработки информации, актуально и для образовательных систем. Защита ИС реализуется путем противодействия угрозам безопасности. В теории защиты информации классифицируют следующие типы угроз, в зависимости от типа воздействия, а именно: нарушение доступа к информации; нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация); несанкционированное тиражирование открытой информации, в нарушение прав ее собственников, в том числе авторских прав; нарушение конфиденциальности информации; нарушение (частичное или полное) работоспособности системы.

В данном случае нами реализуется попытка проектирования обозначенных выше типов угроз на процессы функционирования сферы образования, как достаточно сложной ИС. В частности, в качестве нарушения режима доступа к информации, могут трактоваться действия (или бездействие) персонала образовательных учреждений, приведших к: срыву организации учебного процесса; ограничению коммуникаций преподавателей и обучающихся, путем целенаправленного или непреднамеренного уменьшения объема аудиторной нагрузки (например, с целью экономии фонда зарплаты); некачественная работа всевозможных электронных библиотек, баз данных, средств реализации дистанционного обучения. В свою очередь, студенты, которые пропускают занятия, игнорируют указания по выполнению самостоятельной работы, с использованием, как традиционных средств обучения, так и современных информационно-коммуникационных технологий, препятствуют адекватному осуществлению процессов по достижению цели функционирования – формирования совокупности качественных знаний и умений.

Нарушение целостности информации может проявляться в неполном изложении материала учебных курсов, изменяющем их структуру и, соответственно, искажающем содержание. Такие действия преподавателей могут выражаться в игнорировании требований образовательных стандартов, относительно сущности информации, которую необходимо передать обучающимся, способствующую формированию необходимых профессиональных знаний, умений и навыков. Также может трактоваться, как нарушение целостности информации, формирование знаний, которые не являются актуальными, не соответствуют реальной социально-экономической ситуации и положениям современной научной теории. Несанкционированное тиражирование информации в сфере образования – это использование в учебном процессе и производственной деятельности вузов нелицензионного программного обеспечения, а также элементы плагиата при выполнении студентами рефератов, курсовых и дипломных работ, а сотрудниками – при написании научных статей и подготовке диссертационных работ.

По нашему мнению, вполне уместна и аналогия между действиями преподавателей, сотрудников и студентов в плане нарушения конфиденциальности информации и

работоспособности образовательной системы. Таким образом, нами продемонстрировано как общие подходы в обеспечении информационной безопасности могут быть спроектированы на процессы функционирования вузов и системы образования в целом.

УДК 338.4: 004.9

Ячменева Валентина Марьяновна
д.э.н., профессор
Пушкарева Елена Викторовна
старший преподаватель
Институт экономики и управления
ФГАОУ ВО "КФУ имени В.И. Вернадского"
Республика Крым, Россия

УПРАВЛЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫМ КАПИТАЛОМ ИЛИ КОРПОРАТИВНЫМИ ЗНАНИЯМИ

Интеллектуальный капитал как экономическая категория исследуется на разных уровнях, а именно: на личностном, микроэкономическом и макроэкономическом. Накопление и востребованность интеллектуального капитала является главным условием инновационной модели на всех уровнях. Изменение условий формирования интеллектуального капитала в системах разного порядка, в том числе и региональной системе, требуют от нас поиска новых подходов, логики, принципов и инструментов оценки качества не только внешней и внутренней среды, но и носителей знаний, который чаще всего выступает собственником интеллектуального капитала.

В начале 60-х годов прошлого века концепция человеческого капитала стала новым направлением развития экономической теории. Через некоторое время термин "человеческий капитал" начали использовать социологи, как качественную характеристику населения страны. Важно отметить, что человек как неотъемлемая составляющая этого капитала выступает его носителем, поэтому интеллектуальный капитал, являясь собственностью носителя, зависит от его интеллекта. Справедливо было бы отметить, что на человеческий капитал и его качество было обращено внимание гораздо раньше. Так, после революции, произошедшей в России в 1917 году, первым шагом большевиков было повышение качества жизни населения, то есть его необходимо было постепенно превратить из душевого населения на человеческий капитал. В. И. Ленин понимал, что опыт мирового научно-технического прогресса останется за пределами государства, если не преодолеть неграмотность населения, превратив его из толпы в рабочую силу (для этого везде были организованы кружки ликвидации безграмотности, в то время "ликбез »). Хотя из пропагандистских соображений, с позиции социалистической политэкономии, человеческий фактор не мог рассматриваться, или трактоваться как человеческий капитал, но именно благодаря нему, в течение 70-ти лет на территории Советского Союза при планово-административной системе хозяйствования, было осуществлено множество открытий, достижений. Именно интеллектуальный капитал использовался в период "холодной войны" как оружие противостояния двух социально-экономических систем социалистической и капиталистической. Длительный поединок интеллекта имел положительные и отрицательные результаты, а именно: атомную электростанцию и атомную бомбу, цепную реакцию и водородную бомбу, космос и ракеты с ядерными боеголовками, медицину и штаммы вирусов, сельхозпродукцию и ГМО. Это свидетельствует о том, что развивать человеческий капитал нужно, даже необходимо, но результаты его деятельности должны контролироваться мировым сообществом. Интеллектуальный капитал должен иметь социальное лицо и нести социальную ответственность перед обществом [2].

Итак, формирование, управление, использование и капитализация интеллектуального капитала стали основой новой экономики – "экономики знаний",

которая характеризуется следующими особенностями, где: знания формируют большую часть добавленной стоимости; знания, инновации и творчество являются экономическими категориями; работа со знаниями выделяется в отдельное направление деятельности; коммуникации играют значительную роль и выделяются в отдельную отрасль экономики; иерархическая система управления трансформируется в сложные сетевые структуры.

Исходя из вышеперечисленных особенностей «экономики знаний», менеджеры должны кроме методов управления материальными активами, использовать новые методы управления. К ним относятся методы управления знаниями, талантами, компетенциями, коммуникациями и сетевыми структурами.

Знания, сами по себе, – это результаты интеллектуальной деятельности во всех областях жизни человека. Они имеют ряд специфических свойств: нематериальность; отсутствие физического износа; неисчерпаемость; способность к самовоспроизводству; тиражируемость; доступность. Понятия "знания" и "интеллектуальный капитал" тождественны, поэтому их необходимо понимать шире, чем данные и информация. Интеллектуальный капитал – это все то, что имеет стоимость и является неотъемлемой частью сотрудника компании или формируется в производственных процессах, системах или организационной культуре. Интеллектуальный капитал – это убеждения, моральные ценности, идеи, изобретения, суждения, навыки и профессиональные познания, теории, правила, нормы, системы ценностей, базы данных, методологии, программное обеспечение, бренды, торговые секреты, отношения, мнения, понятия, прошлый опыт и т.д.

Интеллектуальный капитал состоит из человеческого, структурного и покупательского капитала. Структурный капитал - это совокупность технологических, организационных и управленческих знаний, позволяющих эффективно реализовывать производственный потенциал компании. Человеческий (социальный) капитал – это совокупность знаний, практических навыков и творческих способностей сотрудников, направленных на решение задач и достижение целей компании. Покупательский капитал (клиентела) – это совокупность знаний, которые позволяют создать, поддержать и пополнять базу клиентов компании и обслуживать их. Обращаем внимание читателей на то, что многие компоненты интеллектуального капитала не принадлежат компании, они как бы взяты в аренду или лизинг, т.е. являются заемными активами [3].

Таким образом, наличие компетенций, связанных с управлением «нематериальными активами» и с формированием качественно новой инновационной инфраструктуры, является ключевым фактором успеха компаний в повышении ее конкурентоспособности и эффективности [1].

Интеллектуальный капитал состоит из совокупности формализованных и неформализованных знаний, следовательно, на уровне предприятия их можно представить в виде корпоративных знаний.

Формализованные знания – знания, которые можно описать, задокументировать, воспроизвести другим людям. Формализованными, например, являются знания о движении материальных ценностей и процедуре их списания или как служащий может компенсировать понесенные им расходы. Люди могут напрямую передавать друг другу формализованные знания в виде текста, видео, звука, программного обеспечения, кодекса корпоративной культуры и т.д.

Неформализованные знания – продукт личного опыта человека, который отражает его убеждения, моральные ценности и взгляды. Эти знания нельзя увидеть или задокументировать, а передать их можно только вербальным общением. Например, знания передаются в результате наставничества при передаче опыта общения с клиентом, если он агрессивно настроен. Опытный сотрудник приводит случаи из своей практики, излагает подходы, которые выработались в компании в отношении таких клиентов.

При самом общем рассмотрении корпоративные знания можно ориентировочно разделить на несколько категорий:

знание бизнес-процессов компании;
знание корпоративной культуры;
знания о внешней среде компании;
навыки применения информационных технологий (ИТ);
личные знания сотрудников.

Конечно, корпоративные знания – это большой и сложный комплекс информации, форм его проявления множество, и поэтому управление знаниями выступает как многопрофильная задача. Тем не менее, возможности решения этой многопрофильной задачи, как управление знанием существуют.

Основные этапы и направления процесса организации управления корпоративными знаниями:

аудит имеющегося уровня управления знаниями;
разработка схем и форм обмена знаниями между сотрудниками в процессе межличностных коммуникаций;
постоянное применение разнообразных форм обучения персонала для приобретения новых знаний;
внедрение специальных ИТ для управления знаниями;
разработка системы мотиваций приобретения знаний и обмена ими;
организационные изменения.

Конечно же, все вышеперечисленные направления требуют определенных усилий по организационному развитию компании, поддержки руководством организационных изменений и финансирования соответствующих работ, связанных с внедрением системы управления знаниями. Приоритетным из всех перечисленных мероприятий, конечно же, является финансирование и внедрение системы управления знаниями.

Очень часто предприниматели приравнивают интеллектуальный ресурс к инновационным ресурсам, хотя второе является следствием первого.

Интеллект любой организации составляют организационные знания. Структурно организационные знания представляют совокупность практических, теоретических, стратегических, коммерческих и производственных знаний. Они развиваются благодаря знаниям каждого сотрудника и включают весь набор принципов, фактов, навыков, правил и методов, обеспечивающих деловую активность организации и ее кадровый потенциал. Именно знания и компетентность персонала лежат в основе развития организаций и позволяют находить решения возникающих экономических и организационно-управленческих проблем. Поэтому любая стратегия развития предприятия должна предусматривать адекватную концепцию развития человеческого ресурса и максимальное использование знаний и навыков персонала [4].

Любая инновация представляет собой новую комбинацию производственных и интеллектуальных ресурсов. В современной теории экономики знаний выделяют четыре основных группы нововведений.

Первая группа связана с изменениями конечного продукта или услуг.

Вторая группа касается создания новых и совершенствования существующих технологических процессов и оборудования инструментов, материалов и т.п.

Третья группа включает весь комплекс организационно-структурных нововведений, использование новых методов и средств управления.

К четвертой группе относятся все нововведения в области кадровой работы и социально-психологических отношений, совершенствование форм подбора персонала и т.п. [5].

Выводы. История возникновения интеллектуального капитала тесно связана с историей развития человеческого капитала. Определено, что интеллектуальный капитал включает в себя человеческий капитал, структурный капитал и покупательский капитал.

Дальнейшее развитие интеллектуального капитала тесно связано с развитием "экономики знаний" как "корпоративные знания" и направлением "управление корпоративными знаниями".

Новая комбинация производственных и интеллектуальных ресурсов дает возможность получить инновационный толчок в развитии предприятия.

Список использованных источников:

1. Ячменьова В. М. Визначення ступеня зв’язку, узгодженості двох і більше якісних значень ознак людського капіталу / В. М. Ячменьова, О. О. Каменських // Экономика и управление. — 2012. — № 2.— С. 41–48.

2. Ячменьова В. М. Оцінювання якості людського капіталу на мезорівні : [монографія] / В. М. Ячменьова, О. О. Каменських. — Сімферополь : ВД "АРІАЛ", 2014. — 268 с.

3. Шпак Н. Управление корпоративными знаниями: это уже важно! / Николай Шпак // Журнал "Маркетолог". – Москва, №11, 2004. — Режим доступа: http://www.iteam.ru/publications/human/section_55/article_2211/ (27.01.2016)

4. Инновационное развитие: экономика, интеллектуальные ресурсы, управление знаниями / под ред. Б.З. Мильнера. – Ь.: ИНФРА-М, 2010.

5. Лукичева, Л.И. Управление интеллектуальным капиталом / Л.И.Лукичева. – 3-е изд., стер. – М.: Изд-во «Омега-Л», 2010.

УДК 004

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
Межмидинов Азиз Куртвелиевич
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И.Вернадского»

ЗАЩИТА ИНФОРМАЦИИ ПРИ АВТОМАТИЗАЦИИ БЮДЖЕТНОГО ПРОЦЕССА

Постоянное совершенствование бюджетного процесса привело к увеличению функций финансовых органов, повышенным требованиям к качеству и достоверности обрабатываемой информации при значительном увеличении объема обрабатываемых данных. Появление технических ресурсов, специализированного программного обеспечения и наличие специалистов по информационным технологиям позволило автоматизировать бюджетный процесс.

Вопросам автоматизации бюджетного процесса посвящены многочисленные исследования последних лет, среди которых следует отметить работы Т.С. Ремизовой [1] и А.А. Кушбокова [2, 3], посвященные таким актуальным проблемам автоматизации бюджетного процесса как использовании его в качестве инструмента информационно-аналитической поддержки для принятия управленческих решений, а также особенностям автоматизации составления и исполнения бюджета на региональном уровне и анализу и автоматизации информационных потоков.

Предпосылками для создания системы по автоматизации бюджетного процесса являются: 1) возросший объем обрабатываемой информации; 2) повышение требований к качеству и достоверности предоставляемых данных в режиме реального времени; 3) оснащенность компьютерной техникой рабочих мест и наличие локально-вычислительной сети; 4) появление специализированных программных продуктов; 5) наличие специалистов в области информационных технологий.

При автоматизации бюджетного процесса решается проблема защиты информации, обрабатываемой в единой автоматизированной информационно-финансовой системы за счет следующих организационных мер: обеспечения доступными штатными средствами разграничения прав пользователей на доступ к функциям и информации единой автоматизированной информационно-финансовой системы управления бюджетным процессом, серверам, входящим в серверный комплекс системы; организации и проведения резервного копирования баз данных, ведение каталога резервных копий; осуществления комплекса мероприятий по защите информации, в отношении которой устанавливается требование об обеспечении ее конфиденциальности и составляющей государственную тайну, обрабатываемой с использованием средств вычислительной техники в соответствии с требованиями ее защиты от утечки по техническим каналам и от несанкционированного доступа; выбора и реализации методов и способов защиты информации, обрабатываемой и хранимой в единой автоматизированной информационно-финансовой системы управления бюджетным процессом, передаваемой по каналам связи при эксплуатации систем электронного документооборота в единой автоматизированной информационно-финансовой системы управления бюджетным процессом; организации антивирусной защиты персональных компьютеров, серверов; выполнения функций администратора безопасности по обеспечению работы АРМ.

Литература

1. Ремизова Т.С. Автоматизация бюджетного процесса как инструмент информационно-аналитической поддержки для принятия управленческих решений // Финансовая аналитика: проблемы и решения. 2014. № 15. С. 35-41.
2. Кушбоков А.А. Особенности автоматизации составления и исполнения бюджета на региональном уровне // Экономика и управление: анализ тенденций и перспектив развития. 2014. № 10. С. 129-133.
3. Кушбоков А.А. Автоматизация информационных потоков в бюджетной системе // Новое слово в науке и практике: гипотезы и апробация результатов исследований. 2013. № 8. С. 155-159.

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Адарчина Светлана Олеговна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ТУРИСТИЧЕСКАЯ ОТРАСЛЬ КРЫМА В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

Республика Крым – уникальный регион Российской Федерации, в котором соединен мощный природно-климатический, историко-культурный и лечебно-оздоровительный потенциал, являющийся основой для развития курортно-туристической сферы.

В настоящее время, в связи со сложившейся ситуацией в мире, Крым оказался под угрозой информационной войны. Информационная война – это воздействие на гражданское население другого государства путём распространения определённой информации. Она проводится с целью подорвать доверие крымчан к власти, разрушить народное единство. В результате распространяемой дезинформации формируется не соответствующий реальности имидж Крыма как региона, непригодного для туризма, отдыха и восстановления здоровья.

Причину негативного восприятия Крыма в мировом сообществе следует искать в умелом использовании технологий и тактики информационных войн, большой опыт ведения которых имеют западные страны. А информационные технологии в России сегодня во многом отстают от технологического уровня ведущих мировых держав, имеющих превосходство в рекламе туристических услуг и рекреационного сервиса.

Можно выделить ряд проблем, тормозящих развитие туристической отрасли Республики Крым:

1. Политическая нестабильность в Украине.

Водная, транспортная, продовольственная блокады по отношению к республике, лишает ее возможности быть самостоятельным и независимым объектом. Последним толчком стало то, что Украина прекратила подачу электроэнергии, что значительно повлияло на внутренний туризм.

2. Проблема транспортной доступности Республики Крым – является одной из главных проблем.

В текущем году отмечается структурная переориентация пассажиропотока в Республику Крым – с приоритетного ранее ж/д транспорта на автомобильный и авиатранспорт. Государство пытается регулировать цены на авиабилеты, но в летний период они значительно возрастают. Автомобильные перевозки встречают трудности на паромных переправах, некачественных дорогах полуострова, отсутствии гостиничного сервиса, в том числе, мотелей.

3. Среди населения Украины и западных стран происходит разжигание русофобских настроений. Несомненно, такие настроения ведут к ухудшению имиджа полуострова на мировой арене. Крым потерял иностранных туристов, которые переживают за свою безопасность.

4. Введение санкций в отношении крымских предприятий. Отмена их не произойдет в ближайшей перспективе, поскольку основанием для их введения служат решения крымского парламента о национализации собственности, ранее принадлежавшей Украине.

5. Приостановление всех инвестиций в Крым со стороны европейских физических и юридических лиц.

Внутренние проблемы Крыма постепенно решаются, поэтому основная задача, стоящая перед крымчанами в настоящее время - это формирование положительного образа нашего полуострова на мировой арене.

Таким образом, современная имиджевая стратегия Крыма и России в целом должна быть системной, многогранной и наступательной. Она должна включать несколько основных направлений:

- Системный охват все каналов массовых коммуникаций — телевидения, радио, печати, интернет-ресурсов, призванных активизировать в своей работе тему продвижения позитивного имиджа Крыма, с фактами, обоснованными аргументами. В особенности следует обратить внимание на социальные сети, как более конкурентоспособные в сравнении с традиционными средствами массовой информации ввиду системы он-лайн, подразумевающей отсутствие временных и территориальных границ, а также значительную часть которой составляет молодежь. Именно данная аудитория, является ядром современных революционных процессов, в связи с чем именно на нее направлен комплекс информационно-пропагандистской и манипулятивной работы, основной задачей которой является формирование протестных моделей восприятия действующих национальных политических режимов. Для достижения данной цели необходимо систематически размещать в социальных сетях, на телевидении, в поисковых компьютерных системах постоянно обновляемых, в зависимости от сезона, коротких рекламных роликов, каждый из которых посвятить отдельной достопримечательности. Также необходим навигатор по гостиницам, в том числе. частным, с указанием их вместимости, цен, доступа к рекреационным ресурсам и контактам.
- Развитие туризма, пропаганда историко-культурных достопримечательностей страны.
  Каждой туристической фирме, необходимо уделить должное внимание рекламе. Необходим единый туристический портал, который бы содержал в себе всю необходимую информацию о курортно-санаторном комплексе: все официальные сайты, отзывы посетителей и т.д.
- Работа с населением. Необходимо объяснять обществу особенности воздействия информационного оружия, чтобы население было менее конфликтным, чтобы оно было готовым противодействовать данному оружию.
- Выделение финансов на развитие информационных технологий в стране. Разрушение государственного имиджа сегодня — одна из главных возможностей современных информационных технологий, поэтому задача государства — идти в ногу с их развитием и быть готовым дать адекватный ответ любой потенциальной информационной угрозе.

Позитивный имидж Крыма, его репутация в отечественных и зарубежных общественно-политических и деловых кругах могут стать основополагающими факторами продвижения туристической отрасли полуострова на мировом рынке рекреационных и туристических услуг, важнейшим конкурентным ресурсом нашей республики.

Хотелось бы добавить, что для создания и проведения долгосрочной имиджевой политики необходимо не только уделять достаточное внимание безопасности и независимости своей страны, но также эффективно транслировать ценности и символы Крыма в мировое сообщество для создания благоприятного фона для проведения внешней политики и для того, чтобы не позволить нашим противникам одерживать победы в информационном противоборстве.

Список литературы:

1. Имидж России «после Крыма»: парадоксы информационной войны: материалы научной конференции кафедры российской политики факультета политологии МГУ имени М.В. Ломоносова 18 ноября 2014 г. / Под ред. И.А. Василенко. — М.: Издатель Воробьев А.В., 2014. — 100 с.
2. Постановление Совета Министров Республики Крым от 29 июня 2015 года № 358.

УДК 004

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
Аметов Рефат Изетович
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»

ИНСТРУМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АИС В ПЕНСИОННОМ ФОНДЕ

Защита государственного суверенитета, всех государственных служб, является одной из основных задач сохранения государственности в целом. Как пишет В.А. Пенкина, «достижение информационного суверенитета – это очень сложная задача для большинства государств, так как обеспечение безопасности своего информационного пространства вступает в противоречие с группой факторов: 1) процессом информационной глобализации; 2) целями мирового доминирования и ведущимися в его интересах информационными войнами, накал и интенсивность которых быстро растут» [1, с. 125]. В связи с этим является актуальным разработка эффективного инструментария информационной безопасности для государственных служб, в частности, для Пенсионного фонда (ПФ).

Как показывает М.Т. Гильфанов, одним из основных инструментов информационной безопасности является принятие решение об оптимизации информационных потоков [2, с. 53]. Информационный поток измеряется количеством обрабатываемой или передаваемой информации за единицу времени и управлять информационным потоком можно следующим образом: изменяя направление потока; ограничивая скорость передачи до соответствующей скорости приема; ограничивая объем потока до величины пропускной способности отдельного узла или участка пути. Информационные потоки ПФ – это конфиденциальная информация о застрахованном лице или пенсионере, которая может передаваться только по личному запросу застрахованного лица, пенсионера, или по отдельным мотивированным запросам организаций, согласно существующим соглашениям по передаче конфиденциальной информации.

Для обеспечения безопасности от несанкционированного доступа, хакерских атак из Интернета и незаконного копирования данных используется комплекс мероприятий: авторизация доступа к данным, аппаратные средства защиты информации, программный комплекс «Верба» (обеспечивает криптографическую защиту), программа VipNet (шифрует сетевой трафик), межсетевые экраны. Используемый в ПФ аппаратно-программный комплекс «ВЕРБА» предназначен для организации системы защищенного электронного документооборота по передаче сведений о застрахованных лицах в территориальные органы ПФР по телекоммуникационным каналам, а также по сдаче отчетности в органы ФНС. ViPNet Client (Клиент) — это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

Литература

1. Пенкина В.А. Зарубежный опыт формирования информационного суверенитета // Каспийский регион: политика, экономика, культура. 2015. № 3 (44). С. 124-128.
2. Гильфанов М.Т. Дифференцированный инструментарий обеспечения экономической безопасности предприятия // Социально-экономические явления и процессы. 2013. № 10 (56). С. 50-53.

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Загорулько Анна Валерьевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ТУРИЗМА

Сфера туризма и рекреации, которая в своем развитии на сегодняшний день опережает по многим направлениям другие сферы и отрасли экономической и социальной деятельности, играет значимую роль в процессе становления и развития национальной и региональной экономики, перехода от преобладания добывающих и перерабатывающих секторов экономической направленности к высокотехнологическим направлениям и расширению сферы услуг. При этом отрасль туризма подвергается большому количеству разнообразных угроз. В связи со стремительным развитием информационных технологий отдельно отмечают информационные угрозы.

Понятие информационной безопасности туризма рассматривается как состояние защищенности субъектов туристической деятельности от угроз информационного происхождения, сочетающееся с наличием благоприятной для функционирования туристических систем различного уровня информационной среды. А также одним из аспектов информационной безопасности туризма является сбалансированное и безопасное воздействие туристической деятельности на территориальные общественные системы. Вопросы безопасности туризма отражает ГОСТ Р 50644-2009 [1], активного туризма – ГОСТ Р 54601-2011 [2]. Эти стандарты отражают требования физической безопасности туристов, но для информационной безопасности они пока отсутствуют. Особенно проблемы информационной безопасности касаются самодеятельных, неорганизованных туристов, которые, например, в Крыму могут пойти в горы неизвестным маршрутом и попасть в неприятную или опасную ситуацию. В этом случае необходимо проводить оповещение туристов в виде описаний опасных участков горной и прибрежной местности, используя для этого сайты официальных туристических агентств и социальные сети, а также различные предупреждающие щиты.

Туристические компании владеют различной конфиденциальной информацией о своих клиентах (счета, адреса, телефоны, доходы и т.д.). Даже самые незначительные, на первый взгляд, сведения о туристе могут сказать очень много о его привычках, предпочтениях, слабостях, графике дня, и состоянии здоровья, чем могут воспользоваться мошенники. Информационная безопасность туристической фирмы соблюдается только при условии строгого соблюдения норм в области защиты персональных данных. К тому же, туризм – одна из отраслей, активно использующих интернет-оплату. Бронирование и заказ номеров в гостиницах, авиабилетов, экскурсионных услуг и другой инфраструктуры с оплатой онлайн – самое обычное явление в сфере отдыха и туризма. Поэтому одной из самых важных задач туристических организаций является безопасность банковских данных и реализация всех требований PCI DSS (стандарта защиты данных в индустрии платежных карт). Информационная безопасность туристической фирмы, как правило, обеспечивается теми же процедурами и средствами, что и любого другого коммерческого предприятия, но с учетом повышенного количества чувствительных данных и транзакций. Проблемы формирования позитивного имиджа туристических объектов и территорий также могут быть решены в русле обеспечения информационной безопасности туризма. Методы обеспечения информационной безопасности различаются в зависимости от объекта. Для туристической организации основными являются механизмы защиты информации и средства конкурентной борьбы. Для туристов – защищенность информационной среды места временного пребывания.

Литература
1. ГОСТ Р 50644-2009. Туристские услуги. Требования по обеспечению безопасности туристов. М.: Стандартинформ, 2010. 12 с.
2. ГОСТ Р 54601-2011. Туристские услуги. Безопасность активных видов туризма. Общие положения. М.: Стандартинформ, 2012. 8 с.

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
Пасочник Оксана Павловна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЦЕНОВАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА РЫНКЕ НЕДВИЖИМОСТИ

При покупке и продаже жилья принимаемое решение как со стороны продавца, так и со стороны покупателя зависит от степени их осведомленности о ценовой ситуации на рынке, о спросе и предложении, об аналогичных вариантах предлагаемого объекта. Новые правила оформления документов, нестабильность политической и экономической обстановки, слабая информированность о правилах оформления сделки, создают угрозы безопасности для агентов рынка недвижимости.

Цены на недвижимость в Республике Крым и Севастополе начали сильно расти вскоре после присоединения Крыма к России, но высокий спрос продержался всего несколько месяцев. Однако собственники жилья не стали снижать цены в надежде на тех российских граждан, кому запрещен выезд за границу, и не имеющих возможности купить там квартиру или дом. Стоимость недвижимости в Республике Крым часто необоснованно завышена, при этом спрос в разы меньше предложения.

Цены реальных сделок отличаются от цен предложений продаж объектов недвижимости. На Севастопольском и Крымском рынке недвижимости зафиксировано несколько факторов снижения цен. Один из них типичный для регионов Российской Федерации – торг, другой, нетипичный – произведение расчетов за объект недвижимости в национальной валюте по курсу доллара США к рублю ниже, установленному Центральным банком РФ на дату совершения сделки. Второй фактор характерный только для Севастопольского и Крымского рынка недвижимости.

При заключении сделок с недвижимостью в Республике Крым могут возникнуть риски и особенности приобретения. Первый риск – высокий налог с продавца, отсутствующий в Украине: при продаже недвижимости, находящейся менее 3 лет в собственности и сумме сделки, превышающей 1 миллион рублей, необходимо заплатить налог на НДФЛ в размере 13 % от суммы прибыли. Второй риск касается местоположения объекта. Законодательство Украины закрывало глаза на застройку береговой линии, и на сегодняшний день, в процессе реформ, хозяева объектов, построенных ближе 500 м от береговой полосы, могут потерять права собственности. Они стараются поскорее продать недвижимость по привлекательной цене неосведомленному покупателю, что в дальнейшем может создать множество проблем. Третий риск – оформление документов. На рынке жилой недвижимости возникает множество трудностей в основном с оформлением документов на квартиру. Приобретая жилье на вторичном рынке необходимо проверять квартиру на наличие задолженностей на Украине, либо квартира может быть под залогом, что проверить довольно проблематично, т.к. большинство агентств недвижимости этого не делает, а совершение сделки только на доверии может быть опасным.

Современный метод ведения строительства и развитие технологий обусловили появления огромного количества компаний застройщиков на рынке недвижимости в Крыму, причем на данный рынок активно заходят западные инвестиции, поскольку он

имеет большие перспективы, поэтому выбор застройщика также относится к факторам риска.

Как правило, сделки по приобретению недвижимости в Крыму проходят по инвестиционному договору, а не по договору купли-продажи. По инвестиционному договору стоимость недвижимости в Крыму будет ниже, чем по договору купли-продажи. В данном случае застройщик строит на деньги, которые привлекает по инвестиционному договору, поэтому получение готовой квартиры будет зависеть от того, как будут продаваться квартиры в этом доме. Принципиальная разница между договором купли-продажи и инвестиционным договором заключается в том, что в имущественные права по первому покупатель вступает в момент подписания договора, а по второму – в момент предоставления застройщиком справки о стопроцентном инвестировании. И уже на основании этой справки происходит регистрация в БТИ. Но не нужно думать, что инвестиционный договор – это плохо, а купли-продажи хорошо. Главное, что конкретно в нем прописано. Существует определенный риск, что застройщик не закончит строительство, поэтому при заключении инвестиционного договора необходимо учитывать несколько факторов. В первую очередь, штрафные санкции, на случай, если застройщик не сдаст объект в назначенный срок. Как правило, типовой инвестиционный договор уже содержит в себе все необходимые пункты, но, вот, именно на пункт «штрафные санкции» нужно обратить пристальное внимание. Ну и сама просрочка, если это неделя – это одно, если – год, то совсем другое. Во-вторых, в одном из приложений к инвестиционному договору необходимо подробно описать получаемый в итоге объект недвижимости. То есть, какая степень отделки; что на полу, потолке и на стенах; если отделка «под ключ», то, что конкретно должно быть установлено: какая мебель, бойлер – марка и модель, телевизор – марка и модель, вплоть до названия и класса энергосбережения оконного профиля, из которого будут изготовлены окна. Если все это будет прописано в договоре, то покупатель в дальнейшем сможет сэкономить драгоценные нервы и деньги.

Покупателям, приобретающим новостройку, когда уже она сдана в эксплуатацию, необходимо знать перечень документов, которые должен иметь застройщик при заключении первой сделки. В законе № 214-ФЗ все указан перечень соответствующих документов: сведения о застройщике, проектная декларация и сам проект.

При заключении сделок с земельными участками нужно учитывать то, что на территории Крыма введен мораторий на приватизацию земли и республиканской собственности до утверждения схемы размещения объектов инфраструктуры образования, здравоохранения, обороны, безопасности. Эта мера свидетельствует о государственном регулировании и сдерживании повышенного интереса к прибрежным земельным участкам, призвана предотвратить несанкционированное изменение границ земельных участков, неконтролируемую застройку полуострова, в том числе приморских территорий. Из-за невозможности проверки статуса земли невозможна реализация права собственности на дома с земельным участком и земельные участки без строения, оформленные в соответствии с украинским законодательством и подлежащие последующей регистрации уже по российскому законодательству.

Рынок недвижимости в Крыму однозначно перспективен и капиталоемок. С приходом крупных иностранных и российских застройщиков инфраструктура, дороги, сервис и курортные зоны быстро начнут улучшаться, а цены на недвижимость — корректироваться с каждым вновь возведенным объектом. Бросовыми они никогда не будут, но адекватными сегодняшним ожиданиям потребителя, а также экономической ситуации в стране они однозначно станут.

Все, чего сейчас не хватает рынку недвижимости в Крыму для его роста и развития, - это адекватное ценообразование, единая правовая система управления и контроля над сделками и строительством, соблюдение законом установленных сроков по перерегистрации права собственности, наличие достаточного количества узнаваемых банков и предложений по ипотеке.

УДК 004.056.53

Апатова Н. В.
д.э.н., д.п.н., профессор
Халитов А. Р.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

В настоящее время, в связи с большой активностью кибератак наносящих большой ущерб разных видов, информационная безопасность приобретает более высокое значение в экономической безопасности предприятия. Сама безопасность предприятия зависит от многих факторов, самый распространенный путь утечки информации является небрежное обращение со служебными документами, сам порядок хранения и регистрации документов у многих предприятий не выдерживает основных нормативов [1].

Основные угрозы информационной безопасности: случайные действия или непреднамеренные, проявляющиеся в ошибках управлении, плохой поддержке систем защиты; умышленные действия или преднамеренные, незаконное получение важной для предприятия информации и использование её в своих целях, то есть возникающие при существование достаточных для этого условий и факторов. Также их можно поделить по видам, таким как: по статусу и последствиям, по типу, по целям, по характеру возникновения, по месту возникновения, по объекту воздействия, по причине возникновения [2].

Существуют 3 ключевые проблемы, с которыми сталкиваются абсолютно все организации: конкуренты; новые бизнес-модели; сложность средств защиты.

Для обеспечения информационной безопасности предприятия необходимо обеспечить административные, технические и организационные меры. Основной вопрос, который стоит решить организации - это создание максимальной защиты своих данных/, представляющих коммерческий интерес, а также идентификация основного врага, способного наносить наибольшие потери.

Основные средства обеспечения безопасности информации предприятия: защита информации внутри системы, при хранении и пересылке; разработка эффективных алгоритмов защиты от угроз; исключение доступа к информации без согласия её обладателя; своевременное выявление и исключение деструктивных воздействий на информацию.

Все крупные предприятия имеют в своем распоряжении сайты, где они предоставляют свои услуги и информацию, а значит их деятельность подвержена Ddos – атакам. Например, сайт агентства недвижимости, деятельность которого практически полностью осуществляется в сети Интернет, представляет основную ценность предприятия. Лишив сайт работоспособности, злоумышленники могут нанести большие финансовые потери агентству и утрату его клиентов. Решения данной проблемы заключается в поиске услуг компании распределенной сети, работа которой построена с учетом постоянного воздействия большого числа кибератак. Примерами таких компаний - поставщиков услуг, которые удовлетворяют многим из вышеописанных требований, являются «Qrator Labs» и «Лаборатория Касперского».

Можно смело говорить о том, что многие предприятия, находящиеся в информационном обороте, не уделяют должного внимания угрозам, которым подвергается их информационная система, обрекая себя на финансовые потери.

Список литературы:

1. Баутов А.В., Эффективность защиты информации // Электронный ресурс. – Режим доступа: http://wwwBRE.ru/1214.

2. Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. - М.: ИПКИР, 2008. - 485с.

УДК 330

Бакуменко Мария Александровна
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ В СФЕРЕ КОРПОРАТИВНОЙ РЕПУТАЦИИ

Предприятие представляет собой сложную социально-экономическую систему, находящуюся в постоянном развитии и взаимодействующую с внешней средой, параметры которой также меняются с течением времени. Внешняя среда может быть представлена как совокупность источников угроз и благоприятных возможностей для предприятия. Важной задачей руководства предприятия является противодействие возникающим угрозам и обеспечение экономической безопасности предприятия. Рассмотрим термин «экономическая безопасность предприятия» (табл. 1).

Таблица 1.

Определения термина «экономическая безопасность предприятия»

Определение	Источник
«**...экономической безопасностью предприятия** является наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам».	1, с. 102
Экономическая безопасность предприятия — «это состояние защищенности его жизненно важных интересов в финансово-экономической, производственно-хозяйственной, технологической сферах от различного рода угроз...».	2, с. 64
«**...экономическая безопасность предприятия** — это наилучшее состояние экономики предприятия в ряду других определенных состояний, обладающее качествами, способными защитить свой потенциал во всех функциональных зонах деятельности: финансы; маркетинг; производство; персонал; организационная культура и имидж; инновации; инвестиции; информационная сфера; политико-правовая деятельность; экология; силовой блок».	3, с. 19

Все существующие угрозы для предприятия в зависимости от сферы возникновения делят на две категории: внутренние и внешние угрозы. Внешние угрозы возникают за пределами предприятия — во внешней среде. К ним относят [2, с. 65]: - экологические угрозы; - угрозы информационного характера; - брендовые угрозы; - и др. К внутренним угрозам относят [2, с. 65-66]: - действия персонала предприятия, противоречащие его интересам; - утечку или утрату информационных ресурсов (в том числе сведений, составляющих коммерческую тайну); - подрыв делового имиджа (репутации) предприятия у бизнес-партнеров; и др.

Ухудшение корпоративной репутации является одной из наиболее серьезных угроз для предприятия. Последствия данной угрозы могут отразиться на многих аспектах функционирования предприятия. Испорченную репутацию предприятия, как правило, очень сложно восстановить/улучшить, а негативные последствия «плохой» репутации для предприятия часто трудно предусмотреть. В то же время, репутация предприятия зависит от конкретных действий топ-менеджмента и сотрудников предприятия, и поэтому при принятии управленческих решений (в том числе инвестиционных) необходимо руководствоваться принципами этики и корпоративной социальной ответственности.

Литература

1. Шалагин Д. А. Методологические основы формирования экономической безопасности предприятия / Д. А. Шалагин // Вестник БНТУ. — 2009. — № 1. — С. 99-102.
2. Ляшко В. Г. Экономическая безопасность в системе устойчивого функционирования предприятия / В. Г. Ляшко // Известия Тульского государственного университета. Экономические и юридические науки. — 2014. — № 3-1. — С. 61-67.
3. Вишневская О. В. Подходы к формированию концепции экономической безопасности предприятия / О. В. Вишневская // Terra Economicus. — 2011. — Т. 9. № 4. Ч. 2. — С. 18-24.

УДК 330

Бакуменко М. А.
старший преподаватель
Голубев А. А.
магистрант 1 года обучения
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РОЛЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ПРИНЯТИИ ИНВЕСТИЦИОННЫХ РЕШЕНИЙ

В деятельности предприятия важно принимать правильные и эффективные инвестиционные решения, основой для принятия которых может служить полная и достоверная информация о состоянии предприятия и его внешнего окружения, знание основных экономических законов и принципов, методов оптимизации [1].

Информация позволяет предприятиям: – контролировать их текущее состояние; – определять стратегические, тактические и оперативные цели и задачи; – принимать обоснованные и своевременные решения; – координировать действия подразделений в достижении намеченных целей. Под информационными ресурсами понимают весь имеющийся объем информации в информационной системе [1].

Принятое решение должно соответствовать следующим требованиям: – обоснованность; – оптимальность выбора; – правомочность; – краткость и ясность; – конкретность во времени; – адресность; – оперативность выполнения. Эффективным решением является выбор альтернативы, которая будет реализована на практике и внесет наиболее значительный вклад в достижение поставленной цели.

Для принятия обоснованного инвестиционного решения необходим учет совокупности внешних и внутренних факторов, что обуславливает необходимость использования внешней и внутренней информационно-аналитической системы [2].

Внешняя информационно-аналитическая система включает в себя: – информацию нормативно-правового характера федеральных органов государственного управления (законы, указы, постановления); – информацию нормативно-правового характера субъектов РФ; – информацию межотраслевого характера; – законодательство в налоговой сфере; – нормативно-методологическую информацию — стандарты обоснования эффективности инвестиционных проектов; – стандарты внешней финансовой и статистической отчетности предприятия, которые являются формами отражения предполагаемых результатов осуществления инвестиционных проектов. Внутренняя информационно-аналитическая система представляет собой совокупность данных о самом предприятии, реализующем инвестиционный проект: сведения о сотрудниках предприятия и их квалификации; уровне организационно-технического развития предприятия; информация о положении на рынке; сведения о финансовом состоянии предприятия и др. [2].

Для разработки бизнес-плана инвестиционного проекта применяется совокупность внешней и внутренней информации [2]. Необходимо заметить, что достоверность используемой при разработке проектных материалов информации будет в значительной мере определять правильность принятого инвестиционного решения.

Литература:

1. Фаттахов Р. В. О роли информационных ресурсов при поддержке принятия управленческих решений на региональном уровне / Р. В. Фаттахов, Е. И. Иванова, О. Н. Сметанина // Вестник Уфимского государственного авиационного технического университета. — 2007. — Т. 9. № 2. — С. 82-87.
2. Управленческий учет: учебное пособие / Под ред. А. Д. Шеремета. — М.: ИД ФБК-ПРЕСС, 2000. — 512 с.

УДК 330

Бакуменко Мария Александровна
старший преподаватель
Новохатская Дарья Николаевна
магистрант 1 года обучения
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

К ВОПРОСУ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ПРОГРАММНЫХ ПАКЕТОВ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИОННЫХ ПРОЕКТОВ

Для оценки эффективности инвестиционного проекта (ИП), как правило, необходимо привлечь группу специалистов из разных областей экономики, что для предприятия является довольно затратным. Чтобы избежать лишних затрат, фирмы могут осуществить данный анализ самостоятельно, при помощи специальных программных пакетов для оценки эффективности ИП. К основным задачам, решаемым данными программами, можно отнести: – получение комплексной оценки финансового состояния определенного объекта инвестирования; – осуществление анализа производственно-финансовой деятельности предприятия; – создание финансового раздела бизнес-плана ИП; – формирование результирующих таблиц; – расчет показателей эффективности ИП, а также учет рисков и неопределенности; проведение сравнительного анализа эффективности альтернативных ИП; и др. [1].

К наиболее востребованным в настоящий момент программам отечественного производства, предназначенным для оценки эффективности ИП, относят: «Альт-Инвест» (фирма «Альт»), «Инвестор» (фирма «ИНЭК»), а также «Project Expert» (фирма «ПРО-ИНВЕСТ КОНСАЛТИНГ» [2].

«Project Expert» — это целая система разработки финансовых планов и ИП, отвечающая международным стандартам и учитывающая специфику российской экономики. Система «Project Expert» рекомендована как стандарт для разработки планов развития предприятий Министерством экономики РФ и Сбербанком РФ. Программа предназначена для разработки бизнес-планов различных уровней сложности [3]. К недостаткам данного программного пакета можно отнести достаточно большую стоимость лицензии. «Инвестор» — программный продукт, ориентированный исключительно на российский рынок. Программа полностью соответствует российскому законодательству и принятой системе бухгалтерского учета. В основу расчета основных показателей эффективности ИП положена имитационная модель денежных потоков. Программа позволяет решать практически все задачи инвестиционного проектирования. В рамках программного продукта «Альт-Инвест» для расчета показателей эффективности ИП также применяется имитационная модель денежных потоков. Программа ориентирована на использование электронных таблиц. Программный пакет «Альт-Инвест», реализованный с использованием электронных таблиц EXCEL, способен работать в среде таких распространенных табличных процессоров как: SuperCalc 4, Lotus 1-2-3, QUATTRO Pro. Достоинством данного пакета является возможность отобразить сразу всю необходимую информацию на одном экране. Таким образом, изменяя значения тех или иных показателей, аналитик может мгновенно получить реакцию на свои действия [4]. К недостаткам данного программного продукта следует отнести следующее: неудобство работы с таблицами; сложность изменения формул; трудности корректировки данных таблицы; отсутствие развитых средств, позволяющих строить сетевой график [5]. Достаточная сложность вносимых изменений требует определенной квалификации пользователя.

Литература: **1.** Официальный сайт компании ИНЭК [электронный ресурс]. Режим доступа: http://1c.ru/vendors/inec/inec_investor.html. **2.** Пацук Е. Б. Российские информационные системы для малого и среднего бизнеса/ Е. Б. Пацук, Т. Г. Долгова // Актуальные проблемы авиации и космонавтики. — 2014. — № 10. Т. 1. — С. 389-390. **3.** Шаймухаметова Д. В. Программные продукты бизнес-планирования / Д. В. Шаймухаметова, С. Р. Кульмухаметова // Наука, техника и образование. — 2015. — № 11. — с. 82. **4.** Арсенина К. С. Российские программные средства для разработки бизнес-планов / К. С. Арсенина // Инновации, технологии, наука.: Сборник статей Международной научно-практической конференции (3 декабря 2015 г., г. Самара). — В 2 ч. Ч.1. — Уфа: РИО МЦИИ ОМЕГА САЙНС, 2015. — С. 179-181. **5.** Савчук В. П. Оценка эффективности инвестиционных проектов: учебное пособие / В. П. Савчук. — М.: Перспектива. — 2006. — 384 с.

УДК 338

Боднар Алина Валериевна
старший преподаватель
АДИ ГВУЗ ДонНТУ
Донецк, ДНР

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИОННЫХ КОММУНИКАЦИЙ

Деятельность современных предприятий неразрывно связана коммуникационными потоками с информационной средой внутри предприятия и за его пределами. В связи с этим, остро встает вопрос обеспечения необходимого для эффективной деятельности уровня информационной безопасности, который с одной стороны позволит предприятию функционировать и развиваться, с другой, – обеспечит надежность сохранения данных [1].

Информационная безопасность организации определяется целенаправленной активностью ее органов и должностных лиц с использованием разрешенных методов и средств по достижению состояния защищенности информационной среды организации, обеспечивающее ее нормальное функционирование и динамичное развитие [2].

Стандартная модель безопасности состоит из трёх категорий:

- конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность - избежание несанкционированной модификации информации;
- доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

В процессе коммуникации передается информация, которая проходит этап кодирования и декодирования. В данном процессе информация может быть искажена либо перехвачена (рис. 1).

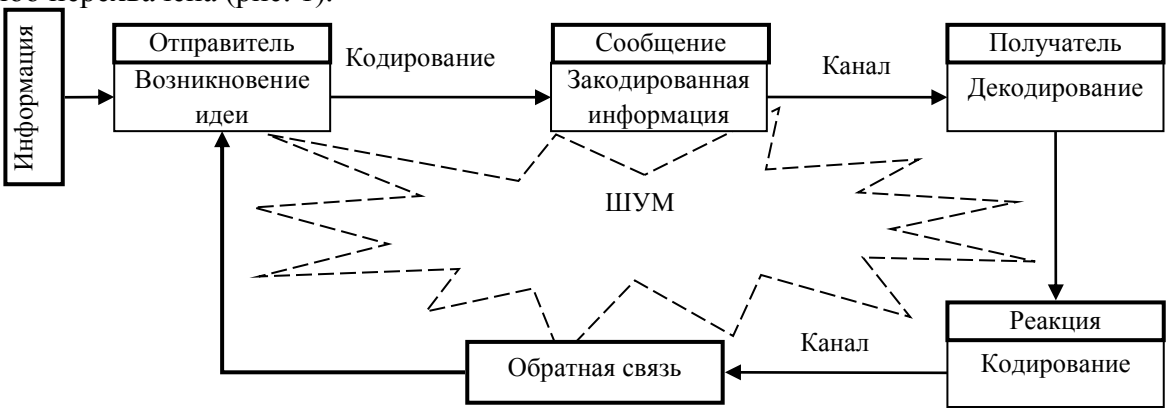


Рис. 1. Коммуникационный процесс с обратной связью

Соответственно, при построении политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты коммуникационного процесса информационной системы: защита объектов информационной системы; защита процессов, процедур и программ обработки информации и каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.); подавление побочных электромагнитных излучений; управление системой защиты.

Таким образом, информационная безопасность организационных коммуникаций является приоритетным направлением повышения эффективности деятельности предприятий различных отраслей экономики и хозяйства.

Список литературы

1. Артамонова Я.С., Артамонов П.А. Информационная безопасность и информационные коммуникации / Я.С.Артамонова, П.А.Артамонов// T-Comm - Телекоммуникации и Транспорт.– М., 2012 - № 12. – С. 69-70

2. Кастельс М. Информационная эпоха: экономика, общество и культура. / М. Кастельс. – М.: ГУ ВШЭ, 2000. – 272 с.

3. Основы программно-аппаратной защиты информации. / М.А.Борисов, И.В.Заводцев, И.В.Чижов. - М.: Книжный дом «ЛИБРОКОМ», 2013. — 376 с.

336.76

Боднер Галина Дмитриевна
к.э.н., доцент
Шинкаренко Светлана Юрьевна
ведущий специалист
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУБЛИЧНЫХ АКЦИОНЕРНЫХ ОБЩЕСТВ РФ

Необходимым условием успешного ведения любого бизнеса является защита коммерческой тайны. В связи с этим проблемы информационной безопасности актуальны для предприятий всех форм собственности. Однако для публичных (открытых) акционерных обществ информационная безопасность особенно актуальна и имеет определенную специфику. В первую очередь это касается акционерных обществ, акции которых обращаются на организованном фондовом рынке.

Неправомерное распространение и использование информации об обществе, его финансовом положении, состоянии корпоративного управления, эмиссионной деятельности и многих других источниках информации способно отрицательным образом повлиять на стоимость акций и активность торгов на фондовой бирже, на результаты хозяйственной деятельности предприятия. Поэтому и в России, и в других странах большое внимание уделяется так называемой инсайдерской информации, обеспечению ее защиты, в том числе и на законодательном уровне.

В Российской Федерации понятие «инсайдерская информация» определено специальным законом от 27 июля 2010 г. № 224-ФЗ и трактуется, как «точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи … и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг, одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов …, либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров) и которая относится к информации, включенной в соответствующий перечень инсайдерской информации…» [2].

К инсайдерам согласно статье 4 указанного закона относятся следующие лица:

- эмитенты и управляющие компании;
- организаторы торговли, клиринговые организации, а также депозитарии и кредитные организации, осуществляющие расчеты по результатам сделок, совершенных через организаторов торговли;
- профессиональные участники рынка ценных бумаг и иные лица, осуществляющие в интересах клиентов операции с финансовыми инструментами, иностранной валютой и (или) товарами, получившие инсайдерскую информацию от клиентов;
- лица, имеющие доступ к инсайдерской информации лиц, указанных в пунктах 1-4 настоящей статьи, на основании договоров, заключенных с соответствующими лицами, в том числе аудиторы (аудиторские организации), оценщики (юридические лица, с которыми оценщики заключили трудовые договоры), профессиональные участники рынка ценных бумаг, кредитные организации, страховые организации;
- лица, которые владеют не менее чем 25 процентами голосов в высшем органе управления лиц, указанных в пунктах 1-4 настоящей статьи, а также лица, которые в

силу владения акциями (долями) в уставном капитале указанных лиц имеют доступ к инсайдерской информации на основании федеральных законов или учредительных документов и другие лица [2].

К инсайдерской информации лиц, указанных в Федеральном законе, относится информация, исчерпывающий перечень которой утвержден Указанием Банка России от 11 сентября 2014 г. №3379-У [1].

В данном документе представлен Перечень инсайдерской информации эмитентов, эмиссионные ценные бумаги которых допущены к торговле на организованных торгах на территории Российской Федерации или в отношении эмиссионных ценных бумаг которых подана заявка об их допуске к организованным торгам. Перечень включает обширную подробную информацию о событиях, касающихся функционирования публичного (открытого) акционерного общества, как эмитента. Информация изложена в 57 пунктах, часть из которых представлена ниже и включает информацию:

- о созыве и проведении общего собрания акционеров эмитента, в том числе о повестке дня, дате проведения, дате составления списка лиц, имеющих право на участие в общем собрании, а также о решениях, принятых общим собранием акционеров эмитента;
- о повестке дня заседания совета директоров (наблюдательного совета) эмитента, а также о принятых им решениях;
- об образовании единоличного исполнительного органа эмитента;
- о появлении лица, контролирующего эмитента, а также о прекращении оснований такого контроля;
- о принятии уполномоченными органами эмитента следующих решений: о размещении эмиссионных ценных бумаг эмитента; об утверждении решения о выпуске (дополнительном выпуске) эмиссионных ценных бумаг эмитента; об утверждении проспекта ценных бумаг эмитента; о дате начала размещения эмиссионных ценных бумаг эмитента; о завершении размещения эмиссионных ценных бумаг эмитента; о направлении (подаче) эмитентом заявления на государственную регистрацию выпуска эмиссионных ценных бумаг, регистрацию проспекта ценных бумаг, государственную регистрацию отчета об итогах выпуска (дополнительного выпуска) эмиссионных ценных бумаг и др.
- о заключении эмитентом договора с российским (иностранным) организатором торговли о включении эмиссионных ценных бумаг эмитента в список ценных бумаг, допущенных к организованным торгам российским (иностранным) организатором торговли, а также договора с российской (иностранной) биржей о включении эмиссионных ценных бумаг эмитента в котировальный список российской (иностранной) биржи;
- информацию, составляющую годовую бухгалтерскую (финансовую) отчетность и консолидированную финансовую отчетность эмитента, а также промежуточную бухгалтерскую (финансовую) отчетность эмитента за отчетный период, состоящий из трех, шести или девяти месяцев текущего года и др. [1].

Таким образом, приведенный в качестве примера выборочный перечень инсайдерской информации охватывает многие аспекты эмиссионной деятельности эмитентов и свидетельствует о том, что при соблюдении требований законодательства по ее защите может быть обеспечена информационная безопасность акционерных обществ.

Список литературы:

1. Указание Банка России от 11 сентября 2014 г. № 3379-У «О перечне инсайдерской информации лиц, указанных в статье 4 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс]. – Режим доступа : http://base.garant.ru/70771550/.

2. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" с изменениями и дополнениями по состоянию на 21.07.2014 г. [Электронный ресурс]. – Режим доступа : http://base.garant.ru/12175530/.

УДК 004.056.56

Бойченко Олег Валерьевич
д.т.н., профессор
Авдошин Иван Александрович
студент 1 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПОЛИТИКА ПРЕДПРИЯТИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности.

Первым элементом политики информационной безопасности (ПИБ) является разработка правового обеспечения защиты информации, представляющая собой систему нормативно-правовых документов, актуальных для деятельности предприятия. В состав правового обеспечения включаются государственные законы и акты, внутренние нормативные и организационные документы предприятия.

Вторым элементом ПИБ является определение потенциальных угроз безопасности информации, которые можно разделить на три группы в щависимости от источника образования:

- случайные ошибки специалистов предприятия при работе с информационной системой и предумышленные действия;
- некорректная работа или отказ технических или программных средств;
- стихийные бедствия и форс-мажорные обстоятельства.

Третий элемент определяет составление перечня данных, подлежащих защите, в состав которого входит открытая информация (ущерб от потери подобного рода сведений не является значительным, поэтому их защита не приоритетна) и закрытая информация (данные, являющиеся государственной тайной — их перечень определяется законодательством; коммерческие или служебные сведения — любая информация, связанная с производством, финансами, использующимися технологиями, утечка или утрата которой может нанести ущерб интересам предприятия; персональные данные сотрудников).

Четвертый элемент определяет создание подразделения, ответственного за вопросы защиты информации. Как правило, на российских предприятиях существует разделение функций, связанных с обеспечением информационной безопасности. Это подразумевает, что за разработку политики защиты данных, выполнение организационных мер отвечает служба безопасности компании, а вопросы, связанные с применением любых программных и аппаратных средств, включаются в компетенцию ИТ-подразделей.

Анализ показывает, что наиболее правильным подходом является создание единой точки принятия решений, а именно создание подразделения, задачей которого будет решение всего спектра вопросов по защите информации на предприятии. В его состав необходимо включить как сотрудников службы безопасности, так и ИТ-специалистов.

Пятый элемент включает определение основных направлений обеспечения информационной безопасности. В рамках решения этой задачи, в частности, обозначаются компоненты автоматизированной системы управления, которые нуждаются в защите, определяются необходимые программные и технические средства, формулируются организационные меры, направленные на защиту информации.

УДК 65.011.12

Бойченко Олег Валерьевич
д.т.н., профессор
Макеева Галина Николаевна
студентка 1 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СПОСОБЫ КРИПТОЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В БЮДЖЕТНОЙ СИСТЕМЕ

В настоящее время, в связи с развитием экономики в сети Интернет способы защиты информационных процессов при помощи криптографического преобразования данных становятся первостепенными в использовании.

При системе бюджетного документооборота через сеть Интернет очень важно защищать информацию от постороннего вмешательства.

Для этого используется современная криптографическая защита, которая включает в себя следующие системы:

- симметричные криптосистемы, отличающиеся тем, что в данных системах используется один и тот же ключ для шифрования[1] и дешифрования[2] (на основании ключа зашифрованный текст преобразовывается в исходный);
- криптосистемы с открытым ключом используют два математически взаимосвязанных ключа - открытый и закрытый. Данный тип защиты зачастую используют при передаче персональных данных через сеть Интернет (информация шифруется с помощью всем доступного открытого ключа, а расшифровывается только с помощью закрытого ключа, известного получателю);
- электронная подпись включает в себя криптографическое преобразование, которое присоединяется к передаваемому тексту, тем самым позволяя другим пользователям проверить авторство и подлинность сообщения.

На всех этапах передачи документов в бюджетном процессе используют последний способ – электронную подпись. Это позволяет вышестоящему и контролирующему органам принимать документы, связанные с финансированием и определять достоверность переданной информации от того или иного ведомства. Также это снижает время на бумажную волокиту и увеличивает скорость принятия документа. Т.е. если ведомство передает запрос на финансирование в контролирующий орган, то ему не надо нести бумажный носитель, достаточно закрепить документ электронной цифровой подписью в программе и передать.

Один из минусов системы информационной защиты в том, что пользователю приходиться носить множество ключей (съемных носителей) от разных программ. Иногда количество может достигнуть 15-20 штук. Для того чтобы устранить эту проблему для ведомств необходимо сгенерировать ключ с цифровой подписью, который будет подходить для некоторых программ сразу. Т.е. организации, занимающиеся IT сферой, заключают договор с Удостоверяющим центром, который сгенерирует один общий ключ для их программ.

[1] Шифрование – это преобразовательный процесс, при котором исходный текст заменяется шифрованным текстом.

[2] Дешифрование – это процесс расшифровывания закодированного исходного текста.

УДК 332.72

Борщ Л. М.
д.э.н., профессор
Зеленюк Ю. С.
студентка 4-го курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РЫНОК НЕДВИЖИМОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ НА ПРИМЕРЕ РЕСПУБЛИКИ КРЫМ

Рынок недвижимости, наиболее актуальная тема для многих научных школ, в том числе и для ученных школы Крымского федерального университета имени В.И Вернадского, таких как Ю.Н. Воробьев, Е.И. Воробьёва С.В. Герасимова, Л.М. Борщ, М.С. Абибуллаев, Г.Г. Ермоленко, М.Ю. Куссый и многие другие. Обсуждаемая тема в настоящее время носит факторный структурный характер в прогнозном моделировании динамики рынка. Объекты недвижимости не только важнейший товар, который удовлетворяет личные нужды людей, но также и капитал в вещной форме, приносящий доход [1]. Развитие рынка недвижимости оказывает существенное влияние на экономическое состояние региона.

Актуальность темы состоит в сложившейся на местном рынке уникальной ситуации – при резко возросшем спросе почти в 13 раз, сделок физически не было из-за длительной перестройки всей регулирующей системы, что дополнительно повышало спрос и, как следствие, цены. Чтобы быть полноценным участником данного рынка, необходимо знать основные особенности его функционирования. Рынок недвижимости Крыма в составе РФ только начал свой этап становления.

Целью данной статьи является анализ динамики рынка недвижимости, выявление закономерностей функционирования рынка недвижимости, определение факторов и особенностей динамики рыночной конъюнктуры.

«Рынок недвижимости – это экономико-правовое пространство, в котором происходит взаимодействие спроса и предложения всех имеющихся на данный момент времени покупателей и продавцов недвижимости и где осуществляется совокупность всех текущих операций с ней» [2].

Рынок недвижимости находится в постоянном развитии и подвержен влиянию внешних политических, экономических, демографических, социальных и прочих факторов.

Структура рынка недвижимости представлена на рисунке 1.

Рис. 1. Структура рынка жилой недвижимости*

*Составлено автором

Первичный рынок – это рынок вновь строящихся объектов и жилья переданного в эксплуатацию. Вторичный рынок недвижимости включает в себя жилье, бывшее в эксплуатации.

Начало 2014 года ознаменовалось политической и социальной дестабилизацией в Украине, что и явилось основным фактором падения цен на рынке. Эти события вызвали падение цен на недвижимость на 2% в начале года. 21 марта 2014 года Крым вошел в состав Российской Федерации, что ознаменовало начало переходного периода, в связи с переходом на российское законодательство и перестройкой всей регулирующей

рынок системы. В новообразованной республике прекратили работу украинские банки, нотариусы, кадастровые и оценочные организации, в то время как российские еще не наладили режим работы. Осложнило ситуацию и то, что Украина закрыла доступ к своему электронному реестру прав собственности на недвижимость. В данных условиях, функционирование рынка оказалось «обесточенным», это второй фактор такого падения, что привело к последующему падению, что и привело к снижению цен на недвижимость на 4% [3].

Наибольшее «замирание» наблюдалось на вторичном рынке жилья, и причина этого не рыночные факторы, а отсутствие государственной регистрации права собственности на недвижимое имущество и сделок с ними в соответствии с законодательством Российской Федерации. Вплоть до августа, вторичный рынок недвижимости находился в состоянии отложенного спроса и предложения [4]. На первичном рынке ситуация была менее критичной. Ранее начатое строительство продолжалось в условиях перехода на новую денежную единицу, повлекшее повышение цен на материалы и заработную плату.

Таким образом, период с марта по август 2014 года, можно охарактеризовать как быстроменяющийся процесс, вызванный резким изменением внешней среды и ценообразующих факторов.

Первая значительная активность на рынке наблюдалась осенью 2014 г., что связано с началом работы Росреестра и, следовательно, реализацией отложенного спроса. Покупательская активность резко увеличилась и цены поднялись на 26% за сентябрь-октябрь [4]. Произошел процесс перерегистрации нотариальных кантор, на территории Крыма заработала банковская система, заработали суды, страховые компании, это и увеличило рост цен. Фундаментальными причинами, этих изменений стали, повышение уровня доходов населения и повышение деловой активности, а социально-психологический стабилизации стал фактором и воздействием отложенного спроса. Таким образом, после резкого повышения цен, большая часть потребителей покинула рынок. Однако продавцы продолжили повышение цен, подняв их еще на 19,5% до конца года. В первые полгода, нахождение крымской недвижимости в составе российского рынка недвижимости, наблюдается «перегрев» рынка, вызванный отложенным предложением и переоценкой ситуации со стороны продавцов. Это, в свою очередь, повлекло безосновательный темп роста цен. По итогам 2014 года, предложение на рынке недвижимости за год уменьшилось на 47%, вместе с тем, средние цены повысились на 46%.

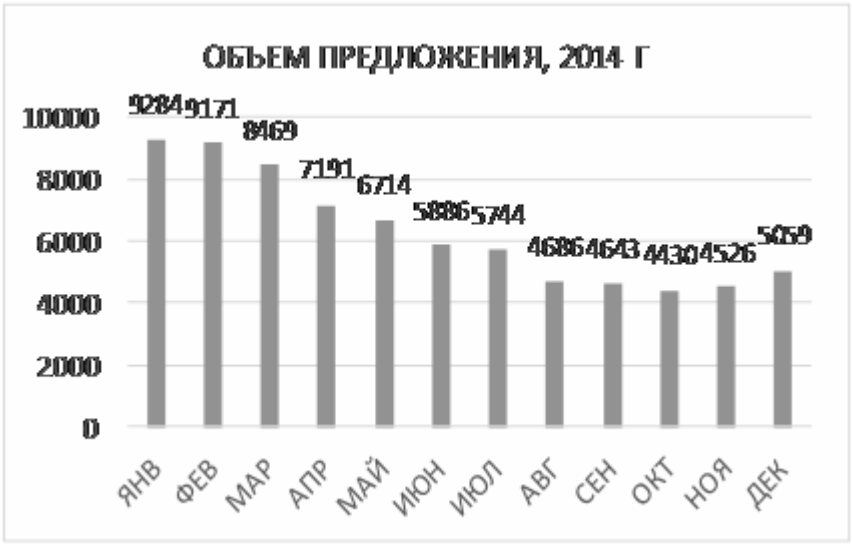


Рис. 2. Динамика объема предложения недвижимости Республики Крым, 2014 г.*

*Составлено автором

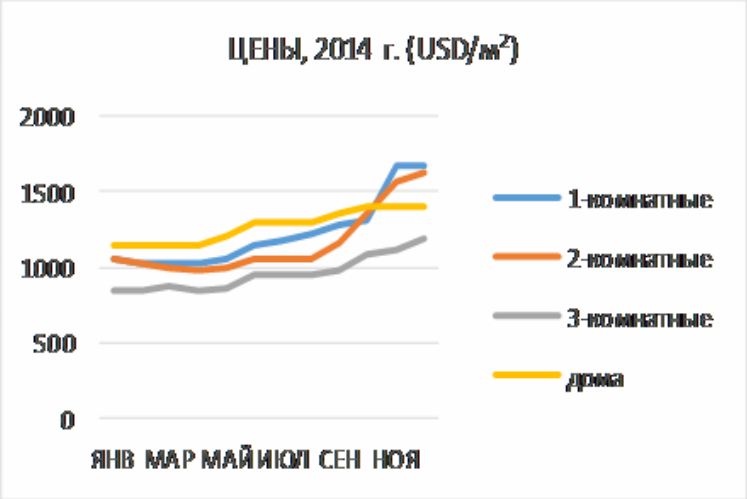


Рис. 3. Динамика цен на недвижимость в Республике Крым, 2014 г.*

*Составлено автором

В январе 2015 года на рынке недвижимости наблюдалась активность, цены остались на прежнем уровне, а объем предложения увеличился. В феврале-марте резко сократилась покупательская способность, несмотря на снижение цен на 17%. В апреле 2015 года снижение цен на недвижимость приостановилось, а объем предложения начал расти. В мае объем предложения увеличился на 16%, цены снизились еще на 2 % и рынок недвижимости достиг равновесного состояния. В июне-июле на крымском рынке недвижимости наблюдался спад активности, характерный для летнего сезона, предложение увеличилось, а цены снизились во всех сегментах рынка на 8%.

В августе 2015 года наблюдались кризисные тенденции российской экономики. Цены на нефть опустились ниже 50 долл./бар, курс рубля почти достиг 70 рублей за доллар, средняя заработная плата снизилась на 9,2%, оборот розничной торговли уменьшился на 8%, ВВП уменьшился на 4,6%.

Данные факторы, оказали негативное влияние на рынок недвижимости в Крыму. В августе объем предложения снизился на 1,4%, цены упали на 2%.

В сентябре 2015 года традиционное сезонное повышение покупательской активности не произошло [5]. Спрос упал еще ниже, предложение незначительно увеличилось, но цены остались на прежнем уровне. Данная ситуация, с неуклонным снижением спроса на недвижимость, должна послужить сигналом для продавцов о необходимости дальнейшего снижения цен [6].

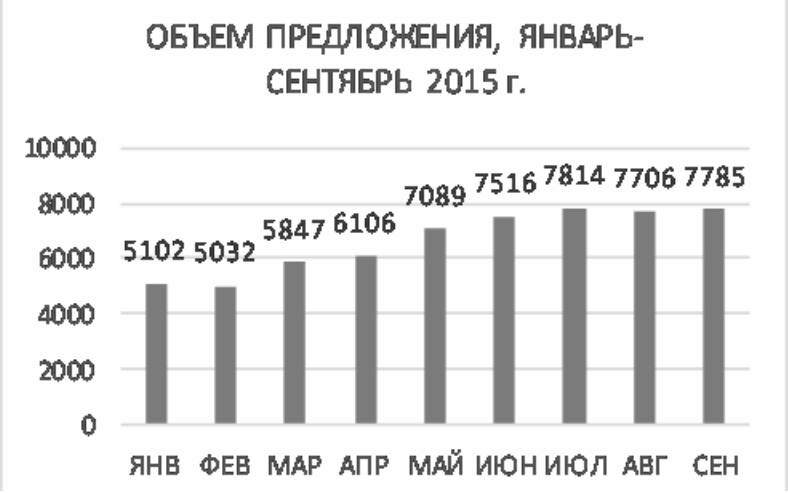


Рис. 4. Динамика объема предложения недвижимости Республики Крым, 2015 г.*

*Составлено автором

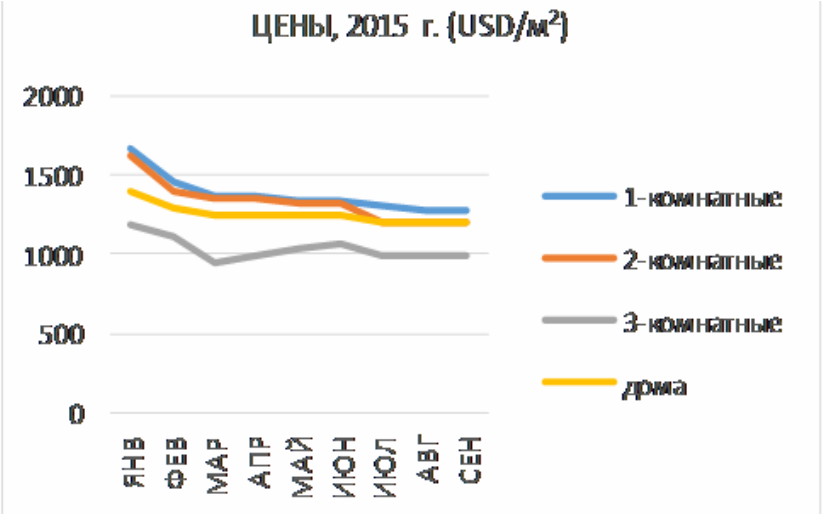


Рис. 5. Динамика цен на недвижимость в Республике Крым, 2015 г.*

*Составлено автором

Рынку недвижимости требуется больше времени для приспособления к изменившимся внешним условиям. В дальнейшем, на рост цен в Крымском Федеральном Округе будет влиять уровень социально-экономического развития. Организация свободной экономической зоны с установлением льготного режима налогообложения, а также строительство моста через Керченский пролив будут оказывать большое влияние на повышение цен на недвижимость в Крыму [7].

ВЫВОДЫ

Во – первых, развитие рынка недвижимости в Республике Крым находится в стадии своего становления, что обусловлено множеством факторов, в том числе происходящими изменениями в экономической и политической ситуации в мире, глобализацией хозяйственных процессов значительными противоречиями и рисками.

Во – вторых, переходный период и вхождение в новом статусе в правовое поле Российской Федерации Республики Крым, как субъекта хозяйствования, санкции влияют и сейчас на процессы и эффективное развитие рынка недвижимости.

В – третьих, снижение темпов роста ВВП повлияло на снижение жизненного уровня жизни населения и падения рынка недвижимости.

Список литературы

1. Воробьёв Ю.Н. Финансовое обеспечение хозяйственной деятельности организаций в условиях нестабильности рынков//Научный вестник Финансы, Банки, Инвестиции. №4(29) 2014. – с. 6-16.
2. Волков Д.Л. Экономика и финансы недвижимости. СПб. 1999 г. – с.32.
3. Воробьёва Е.И. Государственное финансовое регулирование социальных процессов//Научный вестник Финансы, Банки, Инвестиции (№4929) 2014. – с.16-24.
4. Торговая система REM Navigator [Электронный ресурс] // Аналитика. Обзоры цен и рынка недвижимости Крыма. URL: http://remnavigator.com/overview.html
5. Анализ рынка недвижимости для профессионалов. Стерник Г.М., Стерник С.Г.М.: Изд-во Экономика, -2009.
6. Ценообразование на рынке недвижимости в Крымском Федеральном Округе и городе федерального значения Севастополе. Июнь 2014 г. Пичуев Н.Н.
7. А.Н. Асаул, Д.А. Гордеев, Е.И. Ушакова. Развитие рынка жилой недвижимости как самоорганизующейся системы; по ред. засл. строителя РРФ, д-ра экон. наук, проф. А.Н. Асаула. – СПб: ГАСУ. -2008.

УДК 336.717

Борщ Людмила Михайловна
д.э.н., профессор
кафедры финансы предприятий и страхования
Шумейко Вера Игоревна
студентка 4 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРИЧИНЫ ИЗМЕНЕНИЯ ПРОЦЕНТНЫХ СТАВОК ПО ВКЛАДАМ НА РЫНКЕ БАНКОВСКИХ УСЛУГ РОССИИ

Российский рынок банковских вкладов в последние два года активно развивается. Многие банки предлагают разнообразный набор депозитных продуктов. Однако всем известно, что на динамику и объем по вкладам населения особенно влияет размер процентной ставки по этим самым вкладам. Практически каждый день в средствах массовой информации появляются сообщения об изменении процентных ставок по вкладам. Иногда эти ставки повышаются, иногда снижаются. В данных условиях возникает вопрос, что же все-таки влияет на колебания данных процентных ставок. Несомненно, этот вопрос является достаточно актуальным в данное время, т.к. вклады остаются самым популярным средством для сбережения и приумножения доходов населения. Поэтому годовая процентная ставка для большого количества вкладчиков является главным и важным условием при выборе вида банковского вклада. Населению необходимо знать и понимать причины изменения процентных ставок по вкладам, чтобы можно было предвидеть эти самые изменения и не прогадать, положив в банк свои заработанные средства.

Целью данной статьи является раскрытие и изучение основных причин изменения процентных ставок по вкладам на рынке банковских услуг России.

Процентная ставка - это плата, которую заемщик передает кредитору за то, что последний предоставляет первому во временное пользование денежные средства. Несомненно, процентная политика является одним из основных и очень сложных инструментов регулирования банковской деятельности. Основные принципы построения шкалы процентных ставок должны исходить из состояния спроса и предложения на кредитные ресурсы, сроков хранения, величины депозитов, темпов инфляции и т.д.

Банковский вклад – один из наиболее доступных и надежных способов сохранить свои сбережения, защитить от инфляции, а иногда и приумножить их. В настоящее время битва за средства вкладчиков существенно обострилась: банки выводят на рынок новые депозитные продукты, меняют процентные ставки и условия, а Центральный Банк пытается регулировать этот сегмент, вводя новые правила и ограничения. Клиент и банк составляют некий договор о предоставлении банковских услуг (например депозитный договор). По депозитным договорам предметом служит сама сумма, которую клиент кладет на счет и проценты, которые будет выплачивать банком за использование денег.

Процентных ставок имеется столько, сколько и видов вкладов. В каждом банковском договоре, который затрагивает вложение и сохранность денежных средств, прописываются данные об особенностях вклада и сумме, которая будет ежемесячно начисляться клиенту. В результате процентная ставка и есть та сумма, которую банк обязуется выплачивать вкладчику за пользование его финансовыми средствами.

В нынешнее время существует очень много причин изменения процентных ставок по вкладам в банках России. Несомненно, важнейшей причиной является изменение ключевой ставки Центрального Банка Российской Федерации, который устанавливает верхнюю границу доходности банков. Введение ключевой ставки в банковскую сферу произошло в 2013 году и с того времени эта ставка периодически менялась то в сторону повышения, то понижения. На момент введение ключевая ставка составляла 5,5% годовых, ниже этого значения она никогда не опускалась. Пик повышения наблюдался в

декабре 2014 года, когда эта ставка находилась на уровне 17%. На данный момент ключевая ставка составляет 11% годовых. Эти колебания ключевой ставки воздействуют и на процентные ставки по вкладам в банках. В момент, когда произошло резкое повышение ключевой ставки с 10,5% до 17%, многие банки тоже вынуждены были повышать свои ставки по депозитам, однако некоторые достаточно крупные банки приняли позицию выжидания и не стали этого делать. На самом деле у банка есть выбор и право изменять ставки по своим продуктам вслед за изменением ключевой ставки Центробанка или подождать. Однако спустя некоторое, время в силу большой конкуренции на рынке банковских услуг, таким банкам придется выбирать или становиться невостребованным или также повышать свои ставки. И тут мы видим, что на начало 2015 года банковские вклады были самым привлекательным способом формирования сбережений. По итогам первого квартала 2015 года объем вкладов составил 19 трлн. руб. В целом вклады выросли на 2,9%, что, несомненно, связано с высокими процентными ставками, которые повысили банки вслед за повышением ключевой ставки ЦБ. Далее ситуация поменялась, ЦБ снизил ключевую ставку и процентные ставки по депозитам банкам также пришлось снизить, что привело к оттоку количества вкладов. И тут мы видим, что изменение процентных ставок по вкладам на рынке банковских услуг России прямо зависит от изменения ключевой ставки Центрального Банка. Однако это не единственная причина [4].

Еще одной важной причиной изменения процентных ставок банков очевидно является экономическая ситуация в стране, инфляция, санкции, падение рубля и прочие ситуации. Из-за нестабильной экономической ситуации уровень цен на продукты растет, а уровень жизни и доходов населения падает с каждым днем. В условиях, когда маленькая доля потребления базируется на импортных товарах, люди предпочитают потратить рублевые остатки на покупку товаров и услуг. У населения попросту нет свободных денег, которые они бы могли положить в банк. А те, которые располагают такими средствами, попросту боятся вкладывать их в банки, боятся рисковать своими сбережениями, т.к. 2014 и 2015 года стали временем отзыва большого количества лицензий не только у мелких банков, а и у крупных, что сократило суммарный портфель депозитов населения по банковской системе. Тут в свою очередь банки, в силу возросшей конкуренции, нестабильной экономической ситуации и чтобы разжечь интерес у населения к осуществлению вкладов начинают повышать процентные ставки, привлекать население каками-либо бонусами и предложениями, а это отражается высоким риском в случае не достижения населением должного уровня активности. Обычно такими манипуляциями занимаются средние, мелкие банки и на временной основе, т.е. повышенная доходность носит характер разовых акций банков, у которых наблюдается временное снижение объема привлеченных средств. В данной ситуации не стоит забывать, что изменять ставки банки будут в зависимости от уровня ликвидности и поведения текущих вкладчиков (это еще одна причина изменения процентных ставок по депозитам). Сейчас не все банки могут позволить себе устанавливать высокие процентные ставки. В этой ситуации населению стоит забывать, что чем ниже надежность банка, тем выше ставки по депозитам. Обычно это правило работает и играет с населением, которое гонится за высокими процентами, в злую шутку. Поэтому при нынешней экономической ситуации, когда банки пытаются «выжить» в таких условиях, населению нужно внимательнее изучать деятельность банка, а не вкладывать крупные суммы в первый банк (далеко не из первой десятки), предлагающий привлекательные проценты [2].

Выше уже была затронута тема конкуренции на рынке банковских услуг, её тоже нужно выделить как отдельную причину изменения процентных ставок по вкладам. Если в стране высокая конкуренция, то и проценты по депозитам будут меняться. Чем больше банков, тем больше разрыв в предлагаемых вкладчикам цифрах. Здесь нужно так же учитывать, что чем больше в стране банков, тем ниже средний показатель процентной ставки по депозитам и выше по кредитам. Как следствие это плохо сказывается на социальном благополучии населения такой страны. Как пример можно

привести США во времена Великой депрессии. В то время там остались только четыре коммерческих банка, не считая национального. Возможно, именно поэтому Соединенные Штаты стали послевоенным лидером в мире по всем показателям.

Конечно, все мы знаем, что вклады населения в банки – это один из важных способов обогащения этих самых финансовых институтов. И как причину изменения процентных ставок по вкладам можно выделить спрос кредитоспособности. Если этот самый спрос будет достаточно высоким, то банк с легкостью сможет выплачивать невероятно большие по любым меркам проценты по собственным вкладам. Соответственно если снижается спрос на кредитные ресурсы банка, это может привести к понижению процентных ставок по депозитам. И как следствие именно данная связь свидетельствует о низкой ликвидности и затрудненной, из-за разных обстоятельств, платежеспособностью банка. В 2014 году бытовало такое мнение, что банкам просто некуда было вкладывать деньги, привлеченные при помощи депозитов., т.к. ставки были сильно завешены, а спрос на кредит невелик. На тот момент финансовые организации долгое время сохраняли ставки по рублевым депозитам высокими, чтобы привлечь капитал для реализации программ расширения и развития, нужный объем средств в банки давно поступил и был освоен. Излишки просто оседали на балансах, что в не слишком простых экономических ситуациях того времени было не самым лучшим вариантом. Следовательно, необходимо обеспечить так называемый кругооборот и баланс между объемом кредитов и депозитов.

Еще один значимый и немаловажный фактор, от которого зависит депозитная ставка — это начисляемый процент. Всем известно, что проценты бывают простыми (начисляются по истечению срока договора) и сложными (начисляются ежемесячно/ежеквартально и реинвестируются). При данных условиях понятно, что ставка по вкладам со сложными процентами, будет всегда несколько меньше, чем по вкладам с простыми процентами. Однако население чаще отдает предпочтение именно вкладам со сложными процентами. Это объясняется боязнью за свои сбережения, как уже говорилось выше, и надеждой не потерять все и сразу.

Как отдельную причину снижения процентных ставок в летний период 2015 года и как следствие оттока количества вкладов населения можно выделить изменение системы отчислений, которые банки обязаны делать в фонд страхования вкладов. Теперь размер этих отчислений для каждого конкретного банка напрямую зависит от величины ставок по предлагаемым им розничным депозитам. Эти новые правила начали действовать с 1 июля и существенно повлияли на процентную политику банков: если предложенные ими ставки велики, отчисления могут быть увеличены значительно — в разы.

Причины снижения процентных ставок по вкладам в некоторые периоды можно объяснить тем, что в банках закончился сезон новогодних, осенних или как их еще называют сезонных более выгодных для клиентов предложений. Поэтому не обязательно заявлять, что это какая-то тенденция, тем более в те периоды, когда избытка ликвидности на рынке не наблюдалось. В любой ситуации необходимо изучать рынок банковских услуг, как со стороны кредитов, так и депозитов. Т.к. эти операции неразрывно связаны, о чем уже говорилось выше. Тем не менее, этой осенью многие банки отказались от сезонных вкладов, а также сократили количество депозитов. Обычно условия по сезонным вкладам более привлекательны, нежели по стандартным вкладам. Например, проценты по большинству осенних депозитов выплачиваются ежемесячно, половина вкладов имеет возможность пополнения, но меньше трети дают возможность частично снимать денежные средства без потери процентов, что является очень привлекательными особенностями для населения. Такие депозиты обычно невозможно пролонгировать, а кроме повышенных ставок они иногда подразумевают приятные подарки для вкладчиков. Кроме того, банки стараются предложить вкладчикам привлекательные условия досрочного расторжения. Однако на данный момент не все банки могут позволить себе устанавливать высокие процентные ставки. Сейчас средняя ставка по рублевым сезонным депозитам составляет 10,5—11% годовых, максимальная — 13,8% годовых. Это также можно связать с ситуацией Центрального

Банка России, когда в сентябре, а после и 30 октября он принял решение оставить ключевую ставку без изменения на уровне 11 % [3].

Снижение процентных ставок, в любом случае приводит к снижению склонности к сбережению, что, несомненно, отражается на уменьшении реальных темпов роста депозитов. А хорошо это или плохо каждый банк для себя решает сам.

Выводы

Итак, можно подвести вывод и сказать, что любое изменение процентных ставок по вкладам на рынке банковских услуг, прежде всего, будет зависеть от политики ЦБ, в том числе от реализации ряда нормативных инициатив, колебания ключевой ставки ЦБ, уровня инфляции, экономической ситуации в стране, ситуации с ликвидностью на рынке и конечно от конкуренции на рынке банковских услуг. Немаловажной причиной колебания процентных ставок являются и сезонные предложения по депозитам, спектр предлагаемых банком услуг и различные условия по вкладам. Кроме того, ситуация на депозитном рынке будет зависеть и от тенденций рынка кредитования. Вклады населения — все-таки достаточно дорогой источник фондирования, и не все вкладчики намерены брать кредиты под высокий процент. Необходимо регулировать процентную ставку по вкладам в соответствии с экономической ситуацией в стране, уровнем жизни населения и прочими факторами и причинами, которые были рассмотрены в данной статье.

Список литературы

1. Краснова А., Стогней А. Замороженные проценты / А. Краснова, А. Стогней // РБК ежедневная деловая газета. [Электронный ресурс] – 2015. – 14 сент. – Режим доступа: http://www.rbcdaily.ru/finance/562949997145737

2. Лукьянец О. Актуальные процентные ставки по банковским вкладам и прогноз на 2015 год / О. Лукъянец // эксперт Вкладвбанке.ру. – 2015. – 15 мар. – Режим доступа: http://www.vkladvbanke.ru/novosti/02_2015.html

3. Сафронова Ю. Г. Оценка тенденций развития рынка банковских вкладов населения в России [Текст] / Ю. Г. Сафронова, Е. А. Тарханова // Молодой ученый. – 2014. – №8. – С. 585-588.

4. Центральный Банк Российской Федерации [Электронный ресурс]: Режим доступа: http://www.cbr.ru/press/pr.aspx?file=30102015_133001keyrate2015-10-30T13_17_50.htm

УДК 65.011.46: 007

Герасимова Светлана Васильевна
д.э.н., профессор
Бойко Екатерина Владимировна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Сейчас любой производственный процесс не обходится без информационных технологий. Информация для предприятия является одним из важных активов и с каждым разом значимость ее в этом качестве растет. В связи с этим встает вопрос об информационной безопасности на предприятиях.

Информационная безопасность – это защита информации от различных угроз, которые могут быть как случайные или преднамеренные, естественные или искусственные, которые могут нанести вред субъектам информационных отношений, а также владельцам и пользователям этой информации и поддерживающей инфраструктуры [3, с. 11].

Чтобы себя как-то обезопасить, предприятия должны создавать систему защиты информации. Эта система поможет существенно уменьшить материальный ущерб вследствие реализации каких-либо существующих угроз информационной безопасности. Например, Институтом компьютерной безопасности США при участии ФБР был

подготовлен опрос, в котором приняло участие 530 коммерческих и государственных предприятий, понесших ущерб от утечки конфиденциальной информации (более 70 млн. долл.), ущерб от хакерских атак (более 65 млн. долл.), ущерб от вирусов (более 270 млн. долл.) [2].

Таким образом, для предприятия обеспечение информационной безопасности играет важную роль, так как это имеет конкретный экономический смысл. Чтобы создать комплексную защиту информации, нужно определить её инвестиционную эффективность. Она рассчитывается с использованием ряда динамических показателей. При оценке эффективности инвестиций в защиту информации, нужно учесть показатели эффективности этого проекта [4, с. 71]:

- показатели коммерческой эффективности (финансовые последствия реализации проекта по защите информации для его участников);
- показатели бюджетной эффективности (последствия финансирования этого проекта для федерального, регионального или местного бюджета);
- показатели экономической эффективности (что было затрачено и какие результаты, связанные с реализацией этого проекта, выходящие за пределы прямых финансовых интересов участников инвестиционного проекта и допускающие стоимостное измерение).

В качестве основного показателя обычно используют функцию отдачи от инвестиций – ROI [1]:

$$ROI = NPV(R, d) + NPV(C, d), \quad (1)$$

где:

R – денежный поток, который дополнительно создается в результате реализации проекта; C – затраты, которые образовались во время реализации проекта; d – ставка дисконтирования; NPV – функция дисконтирования.

Схематично методологию анализа целесообразности вложений средств в проекты, направленные на обеспечение информационной безопасности можно представить таким образом (рис. 1):

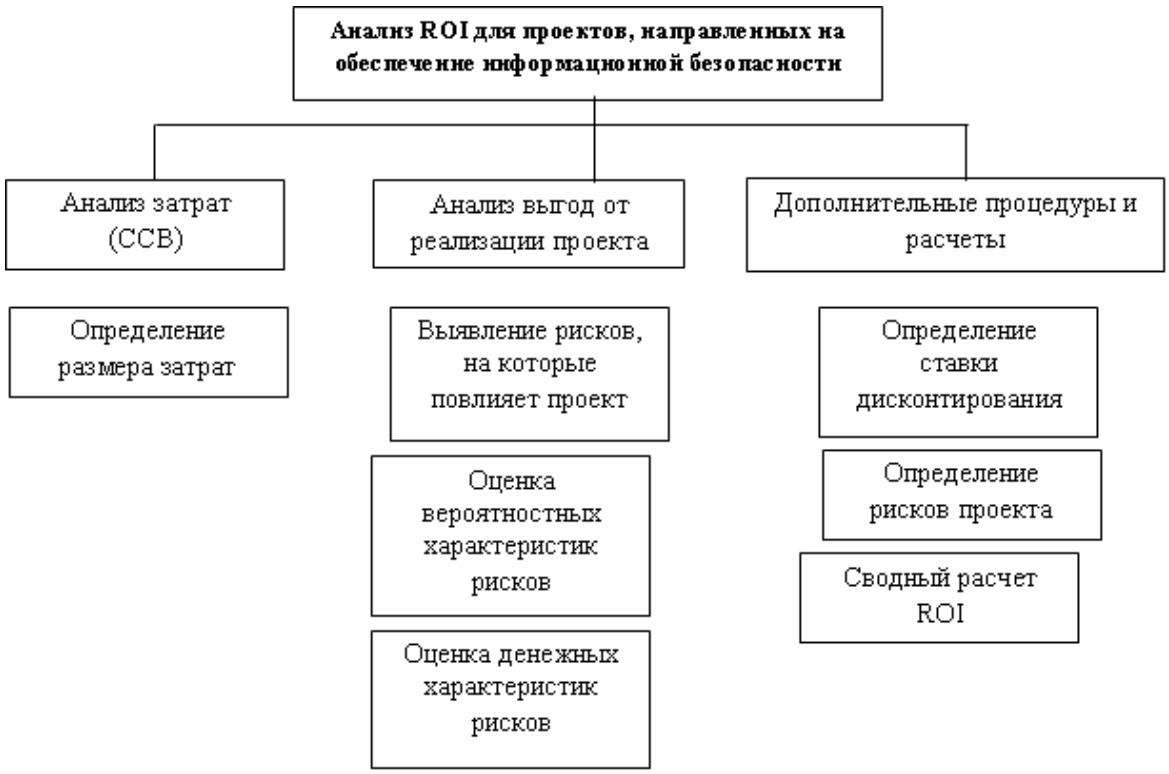


Рис. 1. Структура методологии анализа эффективности вложений в проекты по обеспечению информационной безопасности [1]

Чтобы оценить предстоящие затраты и результаты проекта, оценку эффективности нужно осуществлять в пределах расчетного периода, длительность которого определяется продолжительностью создания, эксплуатации и ликвидации, средневзвешенного нормативного срока службы оборудования, достижения характеристик прибыли, требований инвестора.

Также требуется сравнение нескольких проектов и выбор оптимальных из всех. Для этого используются такие показатели, как [4, с. 72]:

- Чистый дисконтированный доход;
- Индекс доходности;
- Внутренняя норма доходности;
- Срок окупаемости.

Важно учитывать риски при осуществлении проекта связанные с нестабильностью законодательства и экономической ситуации, внешнеэкономический риск, неточность показателей, отражающих динамику технико-экономических показателей и т.д.

Обзор теоретико-методических основ оценки эффективности инвестиций, направленных на обеспечение информационной безопасности предприятия, наталкивает на общий вывод, что довольно трудно оценить целесообразность внедрения системы защиты информации. В частности, уделить внимание необходимо уровню достоверности собранных данных и их качеству. Ожидаемый эффект возможно достичь при условии, что саму оценку и подготовку инвестиционных решений осуществляют грамотные специалисты. Поэтому важно, чтобы руководители предприятия набирали опытных специалистов в данной сфере, так как именно от их работы будет зависеть то, насколько будет эффективной система защиты информации, и какой срок эта система прослужит.

Список использованной литературы:

1. Анисимов А. А. Менеджмент в сфере информационной безопасности: Учебное пособие / А. А. Анисимов. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2009. – 176 с.: ил., табл. – (Основы информационных технологий).
2. Арзуманов С. В. Оценка эффективности инвестиций в информационную безопасность [Электронный ресурс]. // Экономически оправданная безопасность. – 2005. - №1.- Режим доступа: http://www.inside-zi.ru/pages/1_2005/23.html
3. Галатенко В. А. Основы информационной безопасности. Курс лекций. Учебное пособие – 3 изд. / В.И. Галатенко. - М.: Интернет-Университет Информационных Технологий», 2006. -264 с.
4. Ларина И. Е. Экономика защиты информации; Учебное пособие / М.: МГИУ, 2007. – 92с.

УДК 004.056

Иванов Сергей Викторович
к.ф.-м.н., доцент
Хондо Кристина Александровна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ФИНАНСОВЫХ ОРГАНАХ

Особенность работы с автоматизированными системами (АС) в финансовых органах заключается в том, что в данных АС могут храниться объемные и значимые документы, связанные с финансированием, внутренним учетом в организации и персональными данными сотрудников, потеря или разглашение которых является неприемлемой. Для обеспечения безопасности, сохранения целостности данных и бесперебойности работы АС должны соблюдаться четыре базовых принципа: распознавание, противодействие, восстановление и адаптация [3, с. 124]. Для выполнения этих принципов на практике при внедрении АС в финансовых органах

разработчикам и сотрудникам, которые устанавливают и настраивают АС, следует предусмотреть реализацию следующих методов обеспечения информационной безопасности:

1. Отделение базы данных (БД) от системных компонентов и программных модулей путем ограничения прав доступа к каталогу, в котором хранится БД. При этом конфигурацией и системными настройками должно быть предусмотрено, чтобы файл подключения к базе смог подключиться к БД при запуске АС, аутентификации и авторизации пользователей даже при закрытом доступе к папке с базой.

2. Резервное копирование БД и настроек конфигурации АС на другой носитель или ПК с повышенной защищенностью. Данная мера служит для восстановления данных после ошибок пользователей (например, удаления важных документов), системных сбоев, после которых невозможно возобновить нормальную работу системы без ее переустановки и пр.

3. Настройка записи лог-файлов (или их аналогов), в которых записываются все действия пользователей в АС на языке запросов к БД. Эта функция может быть полезна разработчикам системы для отслеживания возможных или уже свершившихся ошибок или сбоев [1, с. 13].

4. Аудит пользователей, который служит для записи информации о действиях пользователей в системе. Фиксируемые события могут записываться как в саму систему в отдельном программном блоке, доступном только для администраторов АС, так и в отдельный файл или отдельную базу данных [2].

5. Настройка прав доступа и изменения данных таким образом, чтобы каждый из пользователей системы имел свой набор рабочих мест, документов, классификаторов и набор действий, которые он может с ними осуществлять (получать доступ, изменять, удалять). Следует отметить, что достаточно важным вопросом в данном пункте является защита персональных данных, которые могут быть занесены в систему [4].

6. Сотрудники, которые осуществляют внедрение и сопровождение АС, должны ознакомиться с правовыми нормами в сфере защиты информации и подписать информационное соглашение о неразглашении и запрете передачи данных третьим лицам.

Таким образом, описанные мероприятия по обеспечению информационной безопасности направлены на то, чтобы при дальнейшем использовании АС не допустить несанкционированное вторжение в систему, выход из строя важных программно-технических компонентов системы, частичную или полную потерю информации.

Список использованных источников

1. Работа в автоматизированных системах бухгалтерского учета для бюджетных учреждений. – Рыбинск: НПО “Криста”, 2010. - 494 с.: ил.

2. Астахов А. Аудит безопасности информационных систем // Искусство управления информационной безопасностью [Электронный ресурс] - 2013. - Режим доступа: http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/audit-bezopasnosti-informacionnyh-sistem

3. Додонов А.Г., Горбачик Е.С., Кузнецова М.Г. Живучесть информационно-аналитических систем в аспекте информационной безопасности // Зб. наук. пр. «Інформаційні технології та безпека». — Вип. 4. — К., 2003.

4. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

УДК 004.056

Королев Олег Леонидович
к.э.н., доцент
Клименко Юлия Геннадиевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ФИНАНСОВЫХ ОРГАНАХ РЕСПУБЛИКИ КРЫМ

Внедрение системы электронного документооборота - неотъемлемая часть в организации работы каждой организации. Под СЭД понимается программное обеспечение, способствующее автоматизации деятельности сотрудников. Основное предназначение – сопровождение документа на протяжении всего его жизненного цикла, поэтому программа должна включать в себя ряд возможностей – создание, изменение, хранение, поиск и передачу информации.

При разработке программы обязательно уделяется особое внимание настройкам доступа и безопасности, но необходимо учесть, что объемная база данных требует соответствующей защиты, так что помимо внутренних настроек программы, обязательно ограничивать доступ с помощью настройки компьютерных сетей, сетевых устройств, операционных систем. Местонахождение сервера, дополнительное оборудование для стабильной работы сервера в экстренные ситуации и доступ к нему заранее определенного персонала является даже более важной частью безопасности, нежели опасность виртуальных атак сервера.

Существуют угрозы повреждения данных, используемых в СЭД как непреднамеренные, так и целенаправленные:

- угроза целостности данных: возможно повреждение, уничтожение или искажение информации;
- угроза конфиденциальности: нарушение конфиденциальности, кража или перехват информации, изменение маршрутов следования;
- угроза работоспособности системы: умышленные атаки, ошибки пользователей, сбои в оборудовании и программном обеспечении.

Методология обеспечения информационной безопасности и стабильной работы системы электронного документооборота заключается в следующем.

Протоколирование действий пользователей позволяет отследить всю историю или выборочные внесения изменений в базу данных. Как правило, история отслеживается для определения закономерности появления ошибок в программе либо для мониторинга действий пользователя от несанкционированного доступа.

Обеспечение и подлинности документов благодаря использованию электронно-цифровой подписи – основному способу шифрования документов на современном этапе. Концепция - существует два вида ключей, «закрытый» и «открытый», первый позволяет зашифровать информацию, он должен находиться только у владельца, второй позволяет расшифровать информацию, он может находиться в открытом доступе. Документ, подписанный ЭЦП дает гарантию того что документ при передаче не был корректирован. Принадлежность подписи можно определить в специальном центре.

Шифрование информации – процесс преобразования открытой информацию в закрытую. Выполняется по строгим математическим алгоритмам. Расшифровать информацию может только пользователь, имеющий ключ.

Резервирование баз данных – периодический процесс копирования элементов конфигурации и базы данных. Служит как профилактика безопасности от полной либо частичной потери данных в базе в результате программного, технологического сбоя либо преднамеренного нанесения вреда базе человеком. Обязательно делается перед установкой обновлений программного обеспечения. Механизм создания резервного

копирования может быть создан как разработчиком СУБД (Microsoft или Oracle) либо непосредственно производителем СЭД.

Законодательное регулирование создает правовое поле в рамках доступности распространения информации, содержит определения основных терминов отрасли, основные положения в Российском законодательстве: «Об электронной цифровой подписи», «Об информации, информатизации и защите информации», «О связи», «О лицензировании отдельных видов деятельности», «Об информации, информационных технологиях и о защите информации». Также существует ряд государственных стандартов порядка ведения документооборота, алгоритмы криптографической защиты информации в ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования», ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

Ограничение прав доступа позволяет настроить права доступа к базе данных или к серверу в целом, контролировать доступ сотрудников к определенной информации. Для этого создается именной профиль пользователя с паролем, и устанавливаются настройки доступа. Некоторые пользователи могут наделяться дополнительными правами, например, для удаления документов, узкий круг сотрудников может наделяться правами администратора для использования расширенных функций, сервисов и возможности настройки системы - администрирования. Для повышения качества безопасности можно ввести статус «забанен» для сотрудников, которые не будут заходить под своим аккаунтом определенное время, например, находиться в отпуске или уволенных, а также настроить механизм блокировки аккаунта при последовательном некорректном вводе логина/пароля при авторизации.

Построение локальной сети с использованием стандартных протоколов построения сетей (модель OSI). Для контроля действий пользователей необходимо организовать домены безопасности на уровне транспортной сети и сервиса электронной почты, установить регистрации попыток пользователей установления соединений вне заданных доменов безопасности, а также протокольную аутентификацию устанавливаемых соединений, настраивать доступ индивидуально каждому сотруднику.

Серверная комната – выделенное помещение, в котором созданы условия для размещения крупного серверного оборудования, соединяется с магистралями и считается средством обслуживания здания. В законодательстве описан ряд технических требований под такие помещения для длительной и бесперебойной работы оборудования, а также система размещения и организации аппаратной комнаты, таким образом, чтоб риск несанкционированного доступа к ней был минимален.

Широкое внедрение компьютеров во все виды деятельности, постоянное наращивание их вычислительной мощности, использование компьютерных сетей различного масштаба привели к тому, что угрозы потери конфиденциальной информации в системах обработки данных стали неотъемлемой частью практически любой деятельности. Защита информации включает в себя кроме технических мер еще и обучение пользователей правилам сетевой безопасности или правильный подбор обслуживающего персонала. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети.

Список литературы:

1. Модели и информационные системы современной экономики. Монография / Апатова Н.В., Бойченко О.В., Герасимова С.В., Пенькова И.В., Сигал А.В., Дюличева Ю.Ю., Иванов С.В., Королев О.Л., Круликовский А.П., Попов В.Б., Рыбников М.С., Солдатов М.А., Акинина Л.Н., Бакуменко М.А. // Под редакцией Н.В. Апатовой. - Симферополь, 2015. – 520 с.

УДК 338.001.36 : 338.23

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Садретдинов Осман Ринаторич
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ПРИМЕНЕНИЕ ПЕРЕДОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ФЕДЕРАЛЬНЫМИ ОРГАНАМИ ГОСУДАРСТВЕННОЙ ВЛАСТИ НА ТЕРРИТОРИИ КРЫМСКОГО РЕГИОНА

Рынок алкогольной продукции в России во все времена занимал значительное место в экономике. Производство и оборот этилового спирта, алкогольной и спиртосодержащей продукции ввиду высокой доходности и быстрого оборота вложенных средств является привлекательным для недобросовестных участников рынка, в связи с чем требует особого внимания со стороны государства.

Федеральным органом исполнительной власти Российской Федерации, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции, функции по контролю, надзору и оказанию услуг в этой сфере, является Федеральная служба по регулированию алкогольного рынка, действующая на основании Постановления Правительства РФ от 24.02.2009г. № 154.

Государственное регулирование алкогольного рынка осуществляется с целью защиты нравственности, здоровья, прав и законных интересов граждан, экономических интересов Российской Федерации, обеспечения безопасности этилового спирта, алкогольной и спиртосодержащей продукции, нужд потребителей в ней, а также контроля за соблюдением законодательства, норм и правил в регулируемой сфере.

Эффективная реализация возложенных на Росалкогольрегулирование задач на современном этапе невозможна без применения инновационных информационных систем. Одной из таких передовых систем является Единая государственная автоматизированная информационная система учета объема производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции (ЕГАИС), которая используется с целью осуществления государственного контроля за объемом производства и оборота указанной продукции.

Главными задачами внедрения системы ЕГАИС во всех субъектах РФ, в том числе Республике Крым и г. Севастополе являются:

- обеспечение полноты и достоверности учета производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции с возможностью уточнения до субъекта РФ, производителя, вида, наименования продукции, крепости, объема, правильности начисления акциза;
- реализация ведения учета импорта этилового спирта, алкогольной и спиртосодержащей продукции с контролем правильности начисления акциза с возможностью детализации до страны происхождения, производителя, поставщика, импортера, вида, наименования продукции, крепости, объема;
- обеспечение ведения учета федеральных специальных марок и акцизных марок с возможностью детализации до организации, осуществляющей производство и оборот алкогольной продукции или импорт алкогольной продукции;
- проведение анализа состояния и тенденций развития производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции на территории РФ и ее регионов;
- затруднение реализации контрафактной продукции за счет проверки сопроводительных документов, удостоверяющих легальность производства и

оборота этилового спирта, алкогольной и спиртосодержащей продукции, между отправителем и покупателем, которая осуществляется в электронном виде.

Статистика показывает, что сегодня Крымский регион занимает одно из первых мест среди регионов России по плотности производителей алкогольной продукции, благодаря размещению на полуострове крупных винодельческих и коньячных заводов. Поэтому для Крыма, несмотря на отсрочку по срокам подключения участников алкогольного рынка к ЕГАИС, внедрение и подключение организаций, осуществляющих деятельность по обороту и розничной продаже алкогольной продукции на территории региона, к ЕГАИС представляет актуальную задачу.

Таким образом, внедрение Росалкогольрегулированием системы ЕГАИС на всей территории РФ является эффективным шагом на пути к снижению количества контрафактной продукции и обеспечению качества и безопасности продаваемой алкогольной продукции.

УДК 004.056.52 : 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Акинина Людмила Николаевна
старший преподаватель
Панченко Игорь Александрович
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Активное формирование информационного общества в нашей стране значительно меняет ситуацию в отношении вопросов, связанных с отбором, систематизацией, хранением и передачей информации и знаний. Внедрение информационно-коммуникационных технологий (ИКТ) обеспечивает широкий доступ всех членов формирующегося информационного общества к переведенной в электронную форму накопленной человечеством информации. Появляется большое число электронных библиотек, которые позволяют надежно сохранять и эффективно использовать разнообразные коллекции электронных документов.

Вместе с тем, существует проблема, что информационные объекты социально-культурной сферы могут подвергаться внешнему информационному воздействию, что может привести к потере достоверности, в результате этого возможны потери знаний и национального культурно-исторического опыта. Риски в области информационной безопасности могут дестабилизировать и даже искажать роль культурно-исторического опыта в развитии общества.

Одним из наиболее востребованных ресурсов Интернет становятся разнообразные библиотеки. Активная глобализация общества, повсеместное возрастание роли ИКТ во всех сферах деятельности человечества требуют наряду с физической охраной информационных объектов поднимать вопросы об информационной безопасности библиотек.

Выделяют четыре основных вида угроз:

- жизни и здоровью персонала;
- среде его обитания (зданию библиотеки);
- обеспечивающим деятельность библиотеки материально-техническим средствам;
- информационным ресурсам.

В современных библиотеках повсеместно применяются разнообразные ИКТ, которые позволяют пользователю реализовать свое конституционное право на

получение информации путем осуществления необходимых действий с использованием Интернет-технологий. Однако через информацию могут распространяться и вредные для человека сведения. Сегодняшние библиотеки, активно применяющие ИКТ, волею злоумышленников могут становиться источником знаний и информации наносящих вред.

Интернет не ограничивает потребителя не временными, не территориальными барьерами. Применяемые в электронных библиотеках технологии доставки до потребителя необходимых ему документов при помощи сети Интернет, ставят проблему перехвата и искажения информации на одно из первых мест.

При рассмотрении информационной безопасности библиотек, необходимо выделить принципы защиты от вредоносной информации и защиты самих информационных ресурсов. В наше время информация считается одним из самых важных ресурсов. С ростом роли информации, технологий и информационных ресурсов в жизни общества, государства и каждого гражданина, вопросы информационной безопасности становиться все более актуальными и делает современное общество зависимым не только от защиты информационных данных, но и защиты от информации.

Для большинства пользователей информационных ресурсов первоочередное значение имеет защита конфиденциальности и целостности личной информации. В то же время, для библиотек важнее всего обеспечить актуальность и доступность информации, при этом сохранив ее целостность и, в некоторых случаях, конфиденциальность, что становиться еще одной проблемной страницей в истории безопасности общедоступных информационных ресурсов. Для решения проблемы информационной безопасности библиотек, целесообразным становиться анализ специфики библиотечного учреждения как субъекта обеспечения информационной безопасности, который связан с особым характером ее деятельности и функциональными особенностями.

Насколько информация доступна, настолько ее легко перехватить, изменить или уничтожить. Действия, представляющие собой угрозу для информации, причиняют различным государствам значительный ущерб.

Обеспечение информационной безопасности для государственных и региональных библиотек (хранилищ информационных ресурсов) на сегодняшний день не мыслима без обеспечения информационной безопасности как самих хранилищ, так и их информационно-коммуникационной инфраструктуры.

УДК 338.24

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Дикий Сергей Александрович
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

СОЗДАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В последнее время развитие современного общества приводит к тому, что на смену традиционному индустриальному обществу приходит общество постиндустриальное, информационное, в центре внимания которого стоят задачи эффективного использования информационно-коммуникационных технологий (ИКТ) и переход к новым методам ведение хозяйственной деятельности. Одной из ключевых проблем перехода является создание условий информационной безопасности в целом, а также вопрос обеспечения комплексной системы обеспечения безопасности информации в системе электронного правительства.

В сложившихся условиях на территории России и Республики Крым существует широкий спектр угрозы безопасности системы электронного правительства, которая представляет собой самую большую информационную базу и систему. Угрозы могут носить различный характер, а именно: внутренний (воздействие на систему электронного правительства со стороны людей, имеющих определенный доступ), внешний (воздействие на систему электронного правительства со стороны внешних пользователей, киберпреступников, киберспецслужб), а также объективные угрозы (утеря информации в результате техногенных катастроф, природных катаклизмов). На основании этого основным приоритетом проектирования системы информационной безопасности для системы электронного правительства является комплексный подход. Система совмещает в себе различные инструменты защиты информации, необходимые для устранения или минимизации угроз безопасности для всех ее составляющих. Единая система гарантирует выполнение поставленных задач по обеспечению информационной безопасности, вытекающих из угроз и нарушений, общесистемной политики безопасности.

Внедрение и применение информационно-коммуникационных технологий является неравномерным в отдельных регионах и различных слоях населения. Регионы со слабой инфраструктурой электронного правительства выпадают из системы информационных, экономических и социальных связей с использованием современных информационных технологий, поэтому на современном этапе важно рассмотреть состояние Республики Крым по готовности к электронному правительству и эффективному функционированию обеспечения информационной безопасности, выработать рекомендации по эффективному развитию Крыма с точки зрения готовности к электронному правительству и внедрению систем обеспечения информационной безопасности.

С целью достижения высокого уровня информационной базы электронного правительства необходимо внедрение комплексной системы обеспечения информационной безопасности. Данная система должна объединить в себе различного рода меры и способы защиты (правовые, технологические, организационные, технические и физически). Правильный подход к организации системы информационной безопасности подразумевает возможность постоянного изменения и развития. Управление жизненным циклом системы информационной безопасности вызвано необходимостью усовершенствования и адаптации под появляющиеся новые источники угроз, инструментов их реализации и изменения законодательства

На настоящем этапе существует 2 основных условия требований системы обеспечения информационной безопасности электронного правительства.
1. Нормативно-правовые акты РФ, которые регламентируют принципы обязательности защиты информации ограниченного доступа, в том числе личных данных пользователей.
2. Обеспечение достаточного уровня доверия, как обычных пользователей, так и организаций, к электронному правительству как к стороне предоставляющей информационные услуги и сведению к минимуму рисков, связанных с использованием информационных ресурсов электронного правительства для всех участников данного процесса.

Уже сегодня можно отметить реальные изменения в направлении создания и активного использования интернет-приемных в органах государственной власти Крыма, публикации и раскрытия информации о государственных закупках, проведении публичных конкурсов на замещение вакансий на государственной службе, также можно отметить высокий уровень защиты данных при работе с системами электронного правительства.

УДК 339.722:519.865

Куссый Михаил Юрьевич
к.э.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Республика Крым, Россия

ТЕКУЩАЯ ВОЛАТИЛЬНОСТЬ КАК МЕРА РЫНОЧНОГО РИСКА

Сейчас финансовые рынки занимают существенную долю в мировой торговле по объему торгов. Международные финансовые рынки являются важнейшими регуляторами многих процессов, протекающих в мировой экономике.

Кроме того, острота проблемы связана с глобальными сдвигами в мировой экономике. Реакция России на санкции со стороны Евросоюза и США существенно изменили уровень влияния американского доллара, юаня и евро на мировую экономику. Активно развиваются страны БРИКС и ШОС, существенно изменяя векторы развития мировых финансовых рынков. Все это привело к полной потере ориентиров в отношении возможной динамики цены на финансовых рынках и связанных с ней рисков (в том числе макроэкономических).

В связи с этим проблема количественной оценки рыночного риска при торговых операциях на финансовых рынках является одной из существенных задач анализа процессов, проходящих на них.

При проведении торговых операций на финансовых рынках экономический агент решает, в первую очередь, следующие задачи оптимизации: заработать максимальную прибыль от сделки; обеспечить минимум рыночного риска при совершении операции.

Решение первой из этих двух задач является достаточно непростой проблемой, так как зависит от множества факторов (размер торгового депозита у экономического агента, сила текущего тренда, сумма транзакционных издержек, и тому подобное). Эта проблема является темой отдельного исследования, и в этой работе рассматриваться не будет.

Остановимся подробнее на задаче минимизации рыночного риска, решение которой также является не простым.

Проблемам рисков в социально-экономических системах уделено достаточное внимание в работах [1-3]. Но вопросы количественной оценки рыночного риска пока не нашли, на наш взгляд, должного отражения в научных публикациях.

Рыночный риск – это совокупный финансовый риск, связанный с торговой деятельностью экономического агента на конкретном финансовом рынке, который измеряется в двух направлениях:

1) Риск получения убытков при торговле на конкретном рынке (для фиксации выбора конкретного финансового рынка используется сравнительная оценка риска при торговле на альтернативных рынках). Алгоритм оценки этого вида риска предполагает наличие некоторой интегральной меры, которая ретроспективно определяет количественно, насколько рынок анализируемого финансового инструмента является рискованным для осуществления торговых операций на этом рынке. Сравнивая количественные значения этой интегральной меры для различных рынков, экономический агент, исходя из субъективного отношения к риску, может сделать наиболее приемлемый для себя выбор рынка из существующих альтернатив.

2) Риск получения убытков по текущей операции на выбранном экономическим агентом рынке.

Рассмотрим понятие текущей волатильности на финансовом рынке, с помощью которой будем решать проблему измерения рыночного риска.

Цены на финансовых рынках, как правило, поставляются пользователям в виде четырехмерного вектор-ряда цен $\vec{P}(t) = \{Open(t), High(t), Low(t), Close(t)\}$ (рис. 1).

Среди практикующих трейдеров такой способ графического представления информации называется японскими свечами.

Здесь Open – цена открытия торгов за период времени Δt; Close – цена закрытия торгов за период времени Δt; High – максимальная цена торгов за период времени Δt; Low – минимальная цена торгов за период времени Δt.

При этом если за период времени Δt, который иногда называют «ценой» японской свечи, Open(t)>Close(t), то свечу окрашивают в черный цвет. А если за период времени Δt Open(t)<Close(t), то свечу окрашивают в белый цвет.

Таким образом, японская свеча – это специфический графический образ, демонстрирующий поведение цены финансового инструмента на рынке, который имеет пять параметров, дающих информацию экономическим агентам о динамике цены за период времени Δt: Open, Close, High, Low и цвет свечи.

Количественные показатели текущей свечи отображают процесс текущего формирования и движения цены на финансовый инструмент за период времени Δt, где Δt – глубина избранного для анализа горизонта (периодичность поступления цен).

При этом четырехмерный вектор-ряд цен $\vec{P}(t) = \{Open(t), High(t), Low(t), Close(t)\}$, представленный в японской свече, более информативен, чем одномерный ряд цен P_t, так как дает больше информации о процессах ценообразования, которые происходили на рынке за период времени Δt.

Цена любой сделки на финансовом рынке – результат текущего консенсуса мнений покупателя и продавца о будущей динамике цены финансового инструмента с учетом доходности и риска и текущих инвестиционных предпочтений экономических агентов, участвующих в сделке. А на инвестиционные предпочтения экономических агентов в значительной мере оказывает их социально-психологические установки, о чем упоминалось выше.

В этом смысле японская свеча за период времени Δt предлагает нам четыре таких консенсуса: Open, Close, High и Low, которые, как показывает практика, крайне редко равны друг другу.

Величина показателя текущей волатильности (CV) зависит от значений четырехмерного вектор-ряда цен $\vec{P}(t) = \{Open(t), High(t), Low(t), Close(t)\}$ и определяется следующим образом:

$$CV = \frac{High - Low}{|Open - Close|} \geq 1 \cdot \quad (1)$$

Модуль в знаменателе формулы (1) учитывает возможность того, что Open может быть как больше, так и меньше Close. В числителе модуль отсутствует, так как всегда High≥Low.

Формула (1) определяет, во сколько раз высота «тела» свечи – в диапазоне цен Open÷Close – меньше высоты «теней» той же свечи – в диапазоне цен High÷Low (рис. 1).

Так, например, «тело» свечи 2 (рис. 1) имеет практически нулевую высоту. Свечи с таким «телом» появляются на экранах мониторов участников торгов, как правило, когда происходит либо смена текущего тренда, либо его коррекция. То есть уменьшение размеров «тела» текущей свечи при росте его «теней» (как это выглядит для свечи 2 на рисунке 1) подает сигнал участникам торгов о том, что текущий тренд снижает темп своего роста, и, возможно следует ожидать изменения тренда на противоположный.

Напротив, свечи, «тело» которых существенно больше «теней» (свеча 1 на рисунке 1), «сообщают» участникам торгов о том, что текущий тренд скорей всего будет продолжаться.

Минимального значения (CV=1) показатель текущей волатильности достигает, когда High-Low=$\left|\right.$ Open-Close $\left|\right.$. При этом свеча принимает форму прямоугольника без «теней».

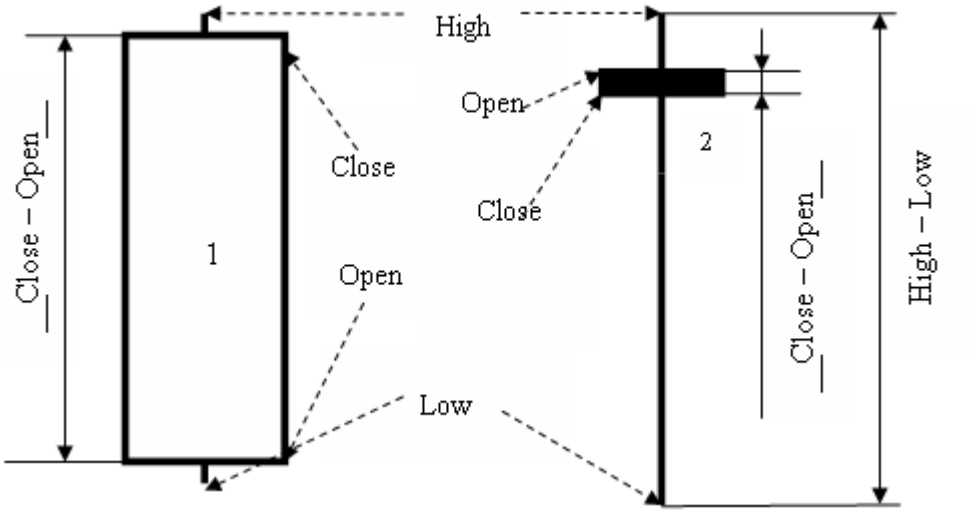


Рис. 1 Представление цены за период времени Δt в виде японских свечей

В рамках сделанного выше допущения CV=1, когда рынок достигает положения своего системного равновесия и динамика цены движется по траектории своего «справедливого» значения от Open к Close.

Социально-экономический смысл CV, рассчитанной по формуле (1), заключается в том, что этот показатель показывает, насколько тренд, действующий в течение исследуемого текущего периода Δt, становится рискованным (непредсказуемым) для продолжения работы в рынке. Чем больше значение CV, тем значительнее различаются мнения участников рынка о соответствии текущего значения цены на исследуемый актив за период времени Δt действующему тренду. Как показали исследования, значение показателя CV начинает существенно превышать единицу, когда на рынке – боковой или вяло текущий тренд, и мнения экономических агентов о будущей динамике цены разноречивы. При этом следует ожидать существенного изменения текущего тренда – ослабления или разворота его – то есть повышения непредсказуемости поведения динамики цены в будущем. При этом увеличивается вероятность риска получения убытков от торговых операций.

Если значение показателя CV уменьшается, то это дает право утверждать, что мнения участников торговли о будущей динамике цены становятся более единодушными, и, как следствие, следует ожидать снижение степени риска получения торговых убытков.

В [4] было показано, что показатель CV можно считать количественной мерой рыночного риска.

Предлагается следующая интегральная мера текущей волатильности финансового рынка:

$$CV_{\text{int}} = \frac{\sum_{i=1}^{n} CV_i}{n}, \qquad (2)$$

где CV_{int} – интегральная мера волатильности рынка, учитывающая глубину исследуемого горизонта (периодичность предоставления цен участникам торгов) Δt;
CV_i – значение текущей волатильности за i-тый период времени Δt;
n – количество анализируемых периодов времени Δt («глубина памяти» рынка). Входной параметр, назначаемый пользователем.

Предлагаемая интегральная мера текущей волатильности финансового рынка представляет собой меру оценки соответствия динамики цены финансового инструмента индивидуальным инвестиционным предпочтениям экономического агента (по отношению к риску). Чем больше величина показателя CV_{int}, тем выше уровень рыночного риска первого вида на анализируемом рынке.

Такая интегральная мера волатильности финансового рынка позволяет адекватно оценить, с учетом индивидуальных инвестиционных предпочтений экономического агента, насколько динамика того или иного финансового инструмента была волатильна за предыдущие n периодов времени Δt на выбранном финансовом рынке. И, если величина CV_{int} окажется слишком большой (слишком малой), по мнению экономического агента, он, при помощи все той же интегральной меры текущей волатильности, сможет выбрать иной финансовый инструмент или иной финансовый рынок, волатильность которого будет соответствовать его инвестиционным предпочтениям (по отношению к риску).

Поскольку показатель CV можно рассматривать (ввиду социально-экономического смысла этого показателя) как адекватную меру количественной оценки текущих психологических настроений финансового рынка, относительное изменение его величины можно использовать как критерий изменения уровня риска получения убытков на финансовом рынке.

Рассмотрим алгоритм применения этого свойства показателя CV в модели, которая может быть описана следующей формулой:

$$MP(\mathrm{t}) = \begin{cases} \begin{cases} \dfrac{\dfrac{1}{m}\sum_{i=1}^{m} CV_{t-i\bullet\Delta t}}{CV_t} > \mathrm{n} \\ \Delta P_t > k \end{cases} & ;\text{начало покупки} \\ \begin{cases} \dfrac{\dfrac{1}{m}\sum_{i=1}^{m} CV_{t-i\bullet\Delta t}}{CV_t} > n \\ \Delta P_t < -k \end{cases} & ;\text{начало продажи} \\ \Delta P_t \text{ меняет свой знак - окончание текуще сделки} \end{cases} \quad (3)$$

где MP(t) – оператор, который переводит из пространства вектор-функции $\vec{\mathrm{P}}(\mathrm{t}) = \{\mathrm{Open(t)}, \mathrm{High(t)}, \mathrm{Low(t)}, \mathrm{Close(t)}\}$ в пространство принятия решений {«покупать», «продавать», «ничего не предпринимать»};

P_t – текущая цена на финансовый инструмент (используется цена $Close_t$);

$P_{t-\Delta t}$ – предыдущая цена на финансовый инструмент (используется цена $Close_{t-\Delta t}$);

ΔP_t – текущее изменение цены на финансовый инструмент: $\Delta P_t = P_t - P_{t-\Delta t} = Close_t - Close_{t-\Delta t}$;

CV_t – текущее значение показателя CV;

n – пороговое значение относительного изменения текущей волатильности CV_t или показатель того, во сколько раз снизилась величина текущего риска получения убытков при осуществлении торговых операций на рынке. Входной параметр (положительное вещественное число), задаваемый пользователем для адаптации модели к уровню волатильности (в смысле CV) рынка;

m – количество свечей, участвующих в расчете, – количественный показатель уровня детерминизма в текущем тренде или глубина «памяти» рынка, который учитывается в расчетах. Входной параметр (натуральное число), задаваемый пользователем для адаптации модели к уровню волатильности (в смысле CV) рынка;

k – параметр, определяющий пороговое значение текущей силы тренда для начала сделки (тангенс угла наклона текущего тренда к оси абсцисс). То есть, для начала сделки текущее изменение цены на финансовый инструмент ΔP_t должна быть по модулю больше k. Входной параметр (положительное вещественное число), задаваемый пользователем для адаптации модели к уровню волатильности (в смысле CV) рынка.

Результаты апробации модели (3) привели к следующим выводам:

• в период высокой текущей волатильности рынка на малых глубинах горизонта (Δt менее нескольких часов) оптимальное значение параметра k: k=0. Для горизонтов с глубиной более суток в период высокой текущей волатильности рынка оптимальное значение параметра k уже становится больше 0 и достигает 10-12 пунктов в зависимости от глубины анализируемого горизонта (пункт равен минимальному изменению цены на финансовый инструмент) и выбранных значений параметров n и m;
• в период невысокой текущей волатильности рынка на разных глубинах горизонта – оптимальное значение параметра k уже становится больше 0. Его величина достигает 10-12 пунктов в зависимости от глубины анализируемого горизонта и выбранных значений параметров n и m.

Общий вывод по параметру k: использование показателя силы тренда k в качестве дополнительного параметра в модели повышает эффективность работы модели (для некоторых значений параметров m и n – существенно), что приводит к повышению рентабельности инвестиций на финансовых рынках;
• значение параметра m («память» рынка), при котором доход от применения модели (3) становится максимальным, не является постоянной величиной и изменяется в диапазоне от 1 до 6 свечей. Следовательно, для анализируемого рынка на каждом из представленных временных горизонтов важно учитывать глубину «памяти» рынка, адаптируя модель (3) с использованием ретроспекции. Проведенный анализ приводит к выводу, что глубина достоверного прогноза (оптимальное значение параметра m) при применении модели (3), как правило, не превышает нескольких свечей, что объясняется идеологией, заложенной в понятие текущей волатильности;
• значение параметра n (текущее изменение величины показателя CV по отношению к его предыдущим значениям — величина текущего риска получения убытков при осуществлении торговых операций на рынке), при котором доход от применения модели (3) становится максимальным, изменяется в диапазоне от 1 до 3. Это значит, что пороговое значение относительного изменения VM (показатель того, во сколько раз снизилась величина текущего рыночного риска) мало. Следовательно, можно учитывать минимальное относительное изменение величины текущего риска получения убытков при осуществлении торговых операций на финансовом рынке.

Рассматривая результаты апробации модели (3) с использованием показателя CV в прогнозном моделировании динамики цены на финансовых рынках можно сделать следующий вывод: показатель CV показал себя как адекватная количественная мера текущего рыночного риска (второй вид рыночного риска), учитывающая инвестиционные предпочтения экономических агентов и их индивидуальное отношение к уровню допустимого риска.

Литература

1. Верченко П. І. Багатокритеріальність і динаміка економічного ризику (моделі й методи): монографія / П. І. Верченко. — К. : КНЕУ, 2006. — 272 с.
2. Економічний ризик: ігрові моделі / В. В. Вітлінський, П. І. Верчено, А. В. Сігал, Я. С. Наконечний / За ред. д-ра екон. наук, проф. В. В. Вітлінського. — К. : КНЕУ, 2002. — 446 с.
3. Королев О. Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О. Л., Малков С. В. // Экономическая кибернетика. — 2013. — № 1-3. — С. 80-85.
4. Ермоленко Г. Г. Выявление зависимости волатильности от энтропии на FOREX / Г. Г. Ермоленко, М. Ю. Куссый, Р. А. Морозов, С. В. Щербина // Культура народов Причерноморья. — 2006. — № 74, т. 2. — С. 16-19.

УДК 336.338

Машьянова Елена Евгеньевна
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПОВЫШЕНИЕ ФИНАНСОВОЙ УСТОЙЧИВОСТИ СТРАХОВЩИКОВ КАК УСЛОВИЕ ДОСТИЖЕНИЯ ИХ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Экономическая нестабильность производственной сферы и низкий уровень доходов населения, сопровождающиеся уменьшением объемов страховых премий у страховщиков, несовершенная законодательная база не создают безопасных условий для устойчивого экономического развития страховой компании. Возникает необходимость в укреплении финансовой безопасности страховщиков и обеспечении стабильности их функционирования. В связи со сложностью и разнообразием внешних и внутренних финансовых отношений возникает потребность в высокоэффективном управлении финансами страховых компаний. Такое управление, прежде всего, обеспечивается благодаря анализу показателей финансовой устойчивости. Именно финансовая устойчивость является одной из важнейших характеристик финансовой безопасности страховщиков с позиции долгосрочной перспективы.

Некоторые ученые рассматривают финансовую безопасность страховщика не как состояние страховой компании, а как процесс достижения определенного состояния страховой компании, которое характеризуется устойчивостью к внутренним и внешним угрозам, оптимальной структурой источников финансирования, обеспечением рационального управления страховыми резервами, своевременным выполнением страховых обязательств и позволяет страховщику производительно функционировать в текущем и будущем периодах.

Недостаточное внимание к роли и месту финансовой безопасности в системе управления страховой компанией приводит к возникновению кризисных явлений, уменьшению уровня ликвидности и платежеспособности, усложняет процесс принятия эффективных управленческих решений и не позволяет обеспечить соответствующий уровень их экономического роста.

Именно в таких условиях руководству страховых компаний целесообразно обратить внимание на сохранение или достижение положительного финансового результата деятельности и сопротивление действиям неблагоприятных факторов. То есть необходимо обеспечить высокую финансовую устойчивость страховщика.

Исследование финансовой устойчивости как экономической категории принадлежит к важнейшим проблемам рыночной экономики, т.к. отсутствие или низкий уровень финансовой устойчивости любого субъекта хозяйствования ведет к неплатежеспособности и, в конечном результате, к банкротству. С другой стороны, слишком высокий уровень финансовой устойчивости будет мешать субъекту хозяйствования осуществлять прибыльную деятельность, обременяя его избыточными запасами и резервами.

Специфика деятельности страховщиков определяется тем, что страховые компании предлагают потребителям услуги, обеспечивающие страховую защиту в виде будущих выплат и возмещений страхователям, которые попали под страховой случай и понесли убытки. Данная особенность функционирования страховщиков («плата наперед») предусматривает необходимость определенных гарантий возможности страховой компании отвечать по своим обязательствам перед страхователями. Поэтому, исходя из природы деятельности страховой компании, исторически выделился основной критерий ее оценки – финансовая устойчивость.

Финансовая устойчивость – это одна из важнейших характеристик поведения любой организации в ситуации внешних и внутренних изменений. От правильности

определения факторов финансовой устойчивости зависит точность количественных и качественных показателей деятельности страховых организаций.

Уровень финансовой устойчивости является главным индикатором жизнеспособности страховой компании и ее возможности выполнять свои финансовые обязательства перед страхователями в условиях негативного влияния разных внешних и внутренних факторов.

Общепринятым подходом к определению финансовой устойчивости страховой компании является ее способность выполнять взятые на себя обязательства по договорам страхования и перестрахования в условиях влияния неблагоприятных факторов.

К основным критериям обеспечения финансовой устойчивости страховщика относятся:

- достаточность собственного капитала;
- уравновешенная тарифная политика;
- сбалансированность страхового портфеля;
- наличие безопасной программы перестрахования;
- адекватные методы формирования страховых резервов;
- оптимальная страховая политика.

На начальных этапах развития страховой компании финансовая устойчивость обеспечивается по большей части размерами и качеством уставного капитала, резервным капиталом, свободными резервами, нераспределенной прибылью. С развитием страховой деятельности растет роль таких факторов, как сбалансированный страховой портфель, тарифная политика, достаточность страховых резервов, перестрахование, инвестиционная политика. От размера собственного капитала зависят возможности страховщика оптимально организовать тарифную, инвестиционную и перестраховую политику.

Финансовая надежность является производной от финансовой устойчивости. Финансово устойчивая страховая компания не всегда будет финансово надежной, потому что надежность зависит от добросовестности и субъективного намерения выполнять свои финансовые обязательства в полном объеме.

Комплексный подход к определению финансовой надежности демонстрирует интегральный показатель $К_н$:

$$К_н = \sqrt[3]{К_л * К_п * К_р} \quad (1)$$

где $К_л$ – коэффициент ликвидности активов;

$К_п$ – коэффициент платежеспособности;

$К_р$ – коэффициент рентабельности страховой деятельности.

Чем выше значение показателя надежности по сравнению со средним показателем по однородной группе страховых компаний, тем выше финансовая устойчивость.

Важнейшей характеристикой финансовой надежности страховой компании является платежеспособность, которая означает способность страховщика при любых обстоятельствах своевременно выполнять денежные обязательства.

Исходя из статей баланса, платежеспособность означает, что стоимость активов страховой компании должна превышать стоимость ее обязательств. Если активы страховщика недоступны в определенное время для осуществления выплат по требованию страхователей – страховщик считается неплатежеспособным. Однако платежеспособность – лишь финансовый признак, а само же понятие «финансовая устойчивость» намного шире и предусматривает наличие определенных условий ее обеспечения.

Источником формирования финансового обеспечения является финансовый потенциал, который представляет собой совокупность финансовых ресурсов страховщика как результат превышения доходов над расходами, с одной стороны, и результатом определенного уровня капитализации, с другой стороны. Финансовый

потенциал развития страховщика – это совокупность свободных от обязательств финансовых ресурсов, которые направляются на расширение деятельности. Он зависит от поступлений страховых взносов, из которых в будущем формируют страховые резервы, от тарифной политики компании, от инвестиционного дохода, от уставного капитала, нераспределенной прибыли и других ресурсов. Поэтому, финансовая устойчивость это не только достаточность финансовых ресурсов, но и наличие финансового потенциала.

Таким образом, можно утверждать, что проблема обеспечения финансовой устойчивости лежит в плоскости эффективного обращения финансовых потоков страховых компаний и выражается в постоянном превышении доходной части над расходами и свободном маневрировании денежных средств путем их рационального использования. Сущность финансовой устойчивости определяется через эффективное формирование, распределение и использование финансовых ресурсов страховой компании.

Подводя итог изложенному, можно сформулировать следующие выводы:

1. Важнейшей составляющей финансовой безопасности страховой компании является финансовая устойчивость, которая означает способность страховщика при любых обстоятельствах своевременно выполнять свои денежные обязательства согласно законодательству и заключенным договорам страхования.

2. Финансовая безопасность страховой компании представляет собой способность страховщика выполнять принятые на себя страховые и другие обязательства при условии обеспечения надлежащего уровня финансовой устойчивости страховой деятельности.

УДК 378.14: 004. 056. 5

Остапенко И. Н.
к.э.н., доцент
Ремесник Е. С.
ассистент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ВУЗ

В век всеобщей информатизации и развития информационно-коммуникационных технологий актуальным является вопрос об информационной безопасности (ИБ). Информационную безопасность система ВУЗ как информационной системы, можно представить в виде двух составных частей: информационно-технической безопасности (ИТБ) и информационно-психологической безопасности (ИПБ).

Отличительной особенностью информационной системы ВУЗ является хранение и обработка большого числа персональных данных профессорско-преподавательского состава, студентов, состав которых постоянно обновляется; данные связанные с обеспечением учебного процесса и особо ценны научно-исследовательские разработки; кроме того конфиденциальные данные организации, служебная информация. Для защиты информационной сферы ВУЗа необходимо создание адекватной политики информационной безопасности. Концепция ИБ основывается на постановлениях, законах правительства Российской Федерации, создании нормативно-правовой базы.

Основная задача – создание собственной системы безопасности, которая учитывает специфику информационной системы ВУЗа. По каждому направлению защиты информации (например, безопасность данных, использование средств криптографической защиты) разрабатываются мероприятия, процедуры по безопасной работе, использование технических средств защиты.

Более подробно коснёмся ИПБ в рамках концепции ИБ ВУЗа. Исходя из свойств информации и законов её преобразования [1], единичный акт информационного взаимодействия объекта со средой можно представить в виде схемы (рис. 1.):

Рис. 1. Акт информационного взаимодействия объекта со средой.

Обеспечение безопасности информации важно на каждом рассмотренном этапе, поскольку информация определяет возможность целесообразного выбора действий субъекта. В случае искажений объект может удаляться от своей цели. Проблема ИПБ требует нового инструментария, отличающегося используемого при решении задач ИБ. Он должен базироваться на методах, учитывающих специфику «субъект-субъектных» отношений, позволяющих исследовать проблемы информационного воздействия на индивидуальное, групповое и массовое сознание.

ВУЗ – открытая система, которая реагирует на внешнюю среду отдельными своими элементами, при этом деление на внешние и внутренние факторы, влияющие на него, условно, так как каждый внешний фактор опосредованно является внутренним, и наоборот. В рамках информационной системы ВУЗ искажения возможные на каждом этапе угрожают его ценностям.

Знание критериев ИПБ ведёт к уменьшению рисков искажения информации. Основные критерии ИПБ (табл. 1.):

Таблица 1.

Критерии информационно-психологической безопасности

Критерий	Источник угрозы ИПБ	Источник получения показателей удовлетворённости
Критерий удовлетворённости личности состоянием ИПБ (информационная недостаточность или информационная избыточность).	Сама информация может быть причиной состояния неопределённости, что ведёт к беспокойству, страху, чувству информационного дискомфорта.	- Опросы, - беседы, - интервью и т.д.
Критерий адекватности отражения личностью окружающего мира (ощущать себя в полной безопасности, хотя его сознание сужено и искажено в результате предшествующих информационно-психологических воздействий).	Информационно-психологические воздействия со стороны различных источников через различные средства воздействия (СМИ, проповедников, пропагандистов и т.д.).	Вера в абсолютные истины в конкретных условиях (несёт в себе потенциальную опасность в случае изменения условий). Формирование научного мировоззрения.

В данном контексте рассмотрим виды угроз (табл.2).

Таблица 2.

Структура угроз ИПБ по источнику возникновения

Виды угроз ИПБ			
Внешние		Внутренние	
Информационная среда	Источники	Информационная среда	Источники
Часть информационной среды общества, которая в силу различных причин неадекватно отражает окружающий мир	Субъекты различной структурно-функциональной организации	Психика человека	Особенности формирования и функционирования психики, индивидуально-личностные характеристики

Меры по безопасности информационно-психологической сферы ВУЗа должны учитывать его публичную сущность, с постоянно меняющейся аудиторией. Кроме того осуществление образовательно-воспитательного процесса достаточно уязвимо с точки зрения ИБ. Рассмотрим основные аспекты преподавания, которые могут нести угрозу ИБ:

1. соответствие преподаваемого материала учебной программе для определенного профиля подготовки, проблемность для данного направления, уровень научности;
2. учет индивидуальных особенностей обучающихся, индивидуальный подход, дифференцирование заданий;
3. этика педагогического общения должна предусматривать не только «сухую» подачу материала, то есть образовательная функция, но и нести воспитательную функцию, психолого-педагогический подход. Учебно-воспитательный процесс намного эффективнее, если преподаватель способствует раскрытию творческих способностей студентов.
4. применение и внедрение нового программного обеспечения, информационных технологий должно быть обосновано с точки зрения педагогического подхода и подкреплено содержанием образовательных программ;
5. контроль и самоконтроль усвоения знаний в процессе и по итогам прохождения дисциплин. Для адекватного оценивания знаний студентов и эффективного протекания учебного процесса необходим промежуточный контроль достигнутых результатов со стороны преподавателя и самоконтроль студентов. Для корректировки занятий при восполнении пробелов в знаниях, навыках, умениях.
6. создание информационно-образовательных ресурсов, соответствующих особенностям ВУЗа и направлениям подготовки, подкрепление учебно-методическими рекомендациями. Встает вопрос о соответствиях стандартам и уникальность материала.

Выявление угроз информационно-психологического характера является «тонкой» задачей. Меры по защите безопасного учебно-воспитательного процесса в основном состоят из психолого-педагогических приемов, соблюдения образовательных стандартов, научности предлагаемой информации, соблюдения правовых норм реализации новых идей и технологий. Своевременное осознание и предотвращение угроз способствует информационной безопасности обучения, в этом случае получаемое образование является конкурентоспособным и отвечающего требованиям современного общества.

Литература:

1. Янковский С.Я. Концепции общей теории информации/ [Электронный ресурс] / С.Я. Янковский //. – Режим доступа: http://bookap.info/okolopsy/teorinf/

УДК 657.1.011.56

Пенькова Инесса Вячеславовна
профессор, д.э.н., профессор
Сейдаметов Ибраим Бекирович
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ФИНАНСОВЫХ ОРГАНОВ МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ

С совершенствованием программно-технического аппарата автоматизированной обработки данных в системе финансовых органов муниципальных образований проблема защиты информации актуализируется. С развитием информационных технологий и их широким внедрением в учетные процессы возникает проблема взаимодействия учетных систем, а также проблема конфиденциальности.

В таких условиях информационные технологии требуют организации высокого уровня защиты данных. Обеспечение требуемого уровня информационной безопасности становится одним из главных условий бесперебойного функционирования финансовых органов [1].

Управление информационной безопасностью позволяет совместно использовать информацию, обеспечивая при этом ее защиту и защиту технических ресурсов. Информационная безопасность состоит из трех основных компонентов [2]: конфиденциальность; целостность; доступность.

Из всего множества способов классификации угроз наиболее подходящей для рассмотрения является классификация угроз по последствиям их влияния на информацию. Основными свойствами информации, определяющие ее ценность, является конфиденциальность, целостность, доступность и предостережение (управляемость).

В автоматизированных системах (АС) различаются следующие классы (виды) угроз информации: нарушение конфиденциальности (уменьшение степени безопасности информации); нарушение логической целостности (нарушение логических связей); нарушение физической целостности (нарушение элементов); нарушения содержания (внешнее навязывание ложной информации); нарушение доступности или отказа в обслуживании; нарушение управляемости; нарушение прав на владение информацией (несанкционированное копирование, использование).

Несанкционированный доступ может осуществляться как с использованием штатных средств, то есть совокупности программно-аппаратного обеспечения, включенного в состав компьютерной системы разработчиком при разработке или системным администратором в процессе эксплуатации, входящих в утвержденную конфигурацию компьютерной системы, так и с использованием программно-аппаратных средств, включенных в состав компьютерной системы злоумышленника. Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения, требуется принятие надлежащих мер предосторожности. В настоящее время существует целый ряд вредных методов, позволяющих использовать уязвимость компьютерных программ по их несанкционированной модификации, с такими именами, как «компьютерные вирусы», «сетевые черви", "троянские кони" и "логические бомбы" [3]. Наиболее эффективным методом борьбы с вирусами представляется использование антивирусного программного обеспечения для предотвращения несанкционированного доступа [4].

Шифрование данных - кодирование информации для ее хранения и передачи по каналам связи. Шифрования (криптография) - один из самых распространенных методов защиты информации в локальных и глобальных сетях. Процесс

шифрования/расшифровки иногда требует затрат времени и аппаратных ресурсов системы, но при этом затрудняет чтение данных при их перехвате [5].

К основным криптографическим методам защиты информации можно отнести: шифрование с помощью псевдослучайных чисел; шифрование с помощью стандартов шифрования данных; шифрование с помощью ключей.

Следует учитывать, что лучшие системы шифрования реализуются в виде аппаратных, программных или программно-аппаратных методов защиты и основаны на специальной аппаратуре, а их стоимость очень высока.

Резервное копирование - необходимая мера для восстановления информации после умышленного или неумышленного повреждения оригинальных данных. Один из действенных методов хранения информации - периодическое копирование данных с последующим хранением за пределами системы. Объектами для резервного копирования могут быть целые диски, отдельные каталоги, файлы [6].

Для повышения надежности систему можно оборудовать устройствами бесперебойного питания и устройствами стабилизации. Эти устройства защищают от пиковых нагрузок в электросети и перепадов напряжения. Подавляющее большинство системы бесперебойного питания функционируют в резервном режиме, а лучшие из них в интерактивном. Процесс переключения на питание от батарей не затрагивает пользователей. При необходимости систему можно оборудовать: устройствами экранирование аппаратуры, линий связи и помещений, в которых находится компьютерная техника; устройствами идентификации и фиксации терминалов и пользователей; средствами защиты портов компьютерной техники и тому подобное.

Таким образом, анализ методов и средств защиты информации показал, что многие специалисты связывают надежность информации в компьютерных системах со средствами их внешней защиты - системой паролей как для входа в компьютерную сеть так и к различным уровням информации системы. А так как круг пользователей, которые имеют доступ к системе хранения/обработки информации может быть достаточно широк (особенно это касается больших систем), то такой подход к защите информации может оказаться малоэффективным. Существенную защиту системы при постоянно растущем риске потери/повреждения информации обеспечивают комплексные методы и средства. Поэтому усовершенствование и внедрение "на опережение" комплексных мероприятий позволит предотвратить несанкционированное использование информации в компьютерных системах.

Список использованных источников

1. Миронов В.В. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» /В.В.Миронов, И.А.Носаль // Информация и безопасность. - 2011. - № 2. - С. 209-211.

2. Осипов В.Ю. Оценка защищенности информационно-вычислительных ресурсов от несанкционированного доступа / В.Ю.Осипов// Приборы и системы управлении. - 1996. - № 7. - С. 16-19

3. Галатенко В.А. Основы информационной безопасности: Курс лекций. Учебное пособие / В.А. Галатенко // Под ред. В.Б. Бетелина. – М.: ИНТУИТ, 2004. – 264 с.

4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. / А.А.Малюк. : Учеб. пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.

5. Ярочкин В.И. Информационная безопасность / В.И.Ярочкин : Учебник для студентов вузов. – 3-е изд. – М.: Академический Проект: Трикста, 2005 – 544 с.

6. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.

УДК 330

Попов В. Б.
к.ф.-м.н., доцент
Кадыров Э. Ш.
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ПРОГРАММНЫЕ МОДЕЛИ ПРОГНОЗИРОВАНИЯ БАНКРОТСТВА ПРЕДПРИЯТИЙ

Актуальность работы. Данная статья касается вопросов прогнозирования банкротств. Проблема прогнозирования финансовой несостоятельности предприятия, и банкротства, занимает в настоящее время лидирующее место среди теоретических и практических проблем управления предприятиями. Россия является страной с развивающейся экономикой, что сказывается на нестабильности многих процессов и факторов, составляющих «внешнюю среду» их деятельности. В результате для обеспечения эффективного управления необходимо не только осуществлять финансовый анализ предприятия в целях определения его состояния на заданном этапе развития, но и проводить раннюю диагностику на предмет возможного банкротства в будущем. Таким образом, выявление неблагоприятных аспектов развития предприятия, прогнозирование кризисной ситуации и банкротства приобретают первостепенное значение.

В последние время ученые пытаются формализовать процесс прогнозирования банкротства компаний и предприятий. Было разработано множество различных математических и математико-экономических моделей. Наиболее широкое распространение в западных методиках прогнозирования риска банкротства нашли модели, разработанные известными экономистами Э. Альтманом, У. Бивером, Р. Лисом и Р. Таффлером. Наиболее известные модели предложены Э. Альтманом, Р. Таффлером и Г. Тишоу, У. Бивером, Г. Спрингейтом , Дж. Фулмером , Томпсоном А.А., А. Стриклендом, Дж. Ольсоном, Ж. Конаном и М. Голдером. В 1972 году появилась еще одна из наиболее популярных ныне моделей – четырехфакторная модель прогнозирования банкротства Р. Лиса. Данная модель была разработана для предприятий Великобритании и включала в себя такие показатели, как: оборотный капитал, прибыль от реализации, нераспределённая прибыль, собственные капитал, заемный капитал и сумма активов. В 1987 году под руководством Ж. Лего была разработана трехфакторная модель (CA-Score) на основе метода дискриминантного анализа. Основным препятствием широкого распространения этой модели помимо ее невысокой точности прогноза (83%), является и то, что она может быть применена только для оценки вероятности несостоятельности промышленных предприятий. В научной литературе отмечается, что с помощью дискриминантных моделей можно диагностировать банкротство с различной степенью вероятности. Так, модель Е. Альтмана позволяет оценить вероятность банкротства за один год с точностью до 95%, за 2 года – 70%, за 3 года – 48%, за 4-5 лет – 30%; модель Л.В. Спрингейта – за год с вероятностью 88-92,5%; модель Дж. Фулмера – за 1 год с вероятностью 98%, за 2 года – 81%. Нужно отметить, что в настоящее время многими зарубежными авторами каждый год предлагаются разнообразные модели прогнозирования банкротства предприятия, основанные как на использовании современных экономико-математических методов (нейросетевых моделей, моделей искусственного интеллекта, построения бинарного дерева классификации BCT – Binary Classification Tree, экспертных оценок и т. д.), так и на расширении набора объясняющих переменных (ВВП, ставка рефинансирования, капитализация компании, отраслевые коэффициенты и др.) Анализируя зарубежные разработки в области прогнозирования вероятности банкротства, следует учитывать, что в связи со сложностями интеграции, попыткой «приспособить» модели к российской

динамичной отчетности, а также неоднозначным толкованием авторами ряда понятий, применяется разное обоснование и дается различный порядок расчета факторов, учтенных в моделях. Российская экономическая наука также исследует проблемы, связанные с оценкой риска банкротства. В частности, авторами наиболее известных методик являются: О. П. Зайцева, А. Д. Шеремет, Г. В. Давыдова и А. Ю. Беликов, и Р. С. Сайфуллин, В. В. Ковалев и О. Н. Волкова, Г. В. Савицкая. Особо отмечается, что среди отечественных моделей диагностики риска банкротства предприятий можно выделить модели, разработанные Р. С. Сайфулиным и Г. Г. Кадыковым в 1996 г. и А. Д. Беликовым и Г.В. Давыдовой учеными Иркутской государственной экономической академии в 1997 г. Достоинством модели Иркутской государственной экономической академии является подробное описание всех основных этапов расчетов, что облегчает применение данной модели на практике. К недостаткам же относят отсутствие отраслевой дифференциации и как следствие несоответствие получаемых прогнозов реальному состоянию.

В 1998 году Зайцева О.П. в работе предложила шестифакторную модель прогнозирования банкротства предприятия. К достоинствам данной модели можно отнести использование шести финансовых показателей, для которых определены нормативные значения, что упрощает процесс интерпретации результатов. Недостатком данной модели является отсутствие методики расчета коэффициентов, что ограничивает возможности использования модели при проведении внешнего анализа. Следующим этапом развития российской методологии анализа угрозы банкротства стала разработка регрессионной модели А.Б. Перфильева, которая использует достаточно большое число переменных, которое равно восьми, что позволяет делать весьма адекватные прогнозы. Одной из последних современных методик прогнозирования банкротства с использованием метода рейтинговой оценки являются модели А. В. Колышкина, предложенные в 2003 году. Автор отобрал показатели, наиболее часто встречающиеся в моделях других ученых и придал им вес. В результате этого у него получилось три статистические модели прогнозирования банкротства. Главным достоинством этих моделей является простота, но, как и в предыдущих случаях, они не всегда дают точные результаты [1-12].

Целью представленной работы является изучение теоретических аспектов банкротства, выявление его причин, видов и признаков, а также рассмотрение отечественных и зарубежных методик оценки вероятности банкротства и методов его предотвращения.

Литература

1. Altman E., Hotchkiss E. Corporate Financial Distress and Bankruptcy: Predict and Avoid Bankruptcy, Analyze and Invest in Distressed Debt, 3rd Edition / E. Altman, E. Hotchkiss // John Wiley and Sons, Ltd. – 2006. – 368 p. – ISBN: 978-0-471-69189-1.
2. Анализ финансового состояния предприятия // Оценка вероятности банкротства // Модель Альтмана (Z модель). Пример расчета [электронный ресурс] http://afdanalyse.ru/publ/bankrostvo/bankrot_1/13-1-0-10 (источник интернет)
3. Altman E.I. Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy // The Journal of Finance. 1968. Sept. P. 589–609.
4. Altman Edward I. Capitalization of Leases and the Predictability of Financial Ratios: A Comment Accounting Review, Vol. 51, No. 2 (Apr., 1976), pp. 408-412.
5. Altman E.I., Haldeman R.G., Narayanan P. Zeta Analysis: A New Model to Identify Bankruptcy Risk of Corporation // Journal of Banking and Finance. 1977. June.
6. Altman E.I. Corporate Financial Distress. New York: John Wiley, 1983.
7. Altman E.I. Further Empirical Investigation of the Bankruptcy Cost Question // Journal of Finance. 1984. Sept. P. 1067–1089.
8. Altman E. Predicting Financial Distress of Companies: Revisiting the Z-Score and Zeta® Models. 2000.
9. Edward I. Altman, Anthony Saunders. Gredit risk measurement; Developments over the last 20 years. Journal of Banking & Finanse 21 (1998) .P. 1721 – 1742.
10. Анализ финансового состояния предприятия // Оценка вероятности банкротства // Модель Таффлера и Тишоу [электронный ресурс] http://afdanalyse.ru/publ/finansovyj_analiz/1/bankrot_tafler/13-1-0-37
11. Beaver William H. Financial Ratios as Predictors of Failure, Empirical Research in Accounting Selected Studies / William H. Beaver // 1966. – Supplement to Journal of Accounting Research. – 4. pp. 71-111.

12. Springate, Gordon L.V. «Predicting the Possibility of Failure in a Canadian Firm» / Gordon L.V. Springate // Unpublished M.B.A. Research Project, Simon Fraser University, January 1978. – 200

УДК 650 : 330

Попов В. Б.
к.ф.-м.н., доцент
Перехрест Р. Д.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

АНАЛИЗ ДОКУМЕНТООБОРОТА В ПЕНСИОННОМ ФОНДЕ РЕСПУБЛИКИ КРЫМ И ЕГО ПОДДЕРЖКА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Современные системы электронного документооборота являются неотъемлемым элементом IT–инфраструктуры. Главная роль систем электронного документооборота заключается в обеспечении оперативной и надежной передачи информации и документации с помощью корпоративных информационных систем. При этом отсутствует необходимость предоставления дубликатов в бумажном виде. Можно вспомнить идеи (которые намного опередили свое время) В. М. Глушкова и его «безбумажную информатику». Электронный документооборот позволяет повысить эффективность деятельности коммерческих организаций и отечественных предприятий. В последнее время можно говорить об автоматизации документооборота в технологических процессах пенсионного фонда Российской Федерации. Инновационные технологии, использующие современные информационные технологии, способствуют незамедлительному решению задач во внутреннем управлении, межведомственном взаимодействии и сотрудничестве с населением. Анализируется поток документации в пенсионном фонде Республики Крым. В качестве основы автоматизации технологического процесса потока документации используется технология ViPNet.

Цель данной работы дать общее представление о технологии ViPNet, рассмотреть основные её функции при использовании на предприятии и описать возможные варианты внедрения ViPNet в зависимости от конфигурации VPN в корпоративных сетях пенсионного фонда Республики Крым. На сегодняшний день, учитывая уровень развития информационных технологий, защита информации любой компании, а тем более государственного учреждения имеет одно из первостепенных значений.

В данной работе рассмотрены эффективные средства создания защищенной и отказоустойчивой виртуальной сети любого масштаба. Гибкое сочетание компонентов ViPNet и их функциональных возможностей позволяет удовлетворить любые потребности как небольших компаний, так и крупных коммерческих и государственных организаций, имеющих территориально распределенные сети.

Защита информации с помощью технологии ViPNet организована, в частности, в органах Пенсионного фонда Российской Федерации (ПФР). Технология обмена электронными документами в системе защищенного электронного документооборота ПФР (далее – СЭД ПФР) по телекоммуникационным каналам связи предназначена для организации защищенного юридически значимого электронного документооборота между Абонентами СЭД ПФР и органом ПФР. Технология обмена электронными документами в СЭД ПФР описывает порядок подключения Абонентов и их взаимодействия с органами ПФР, порядок обеспечения защиты информации и поддержания в актуальном состоянии ключевой документации, описывает компоненты СЭД ПФР и их взаимосвязь. Система защищенного электронного документооборота органов ПФР с Абонентами СЭД по телекоммуникационным каналам связи включает следующие основные компоненты:

- АРМ Абонента СЭД.

- АРМ специалиста органа ПФР.
- Удостоверяющие центры с установленными доверительными отношениями.
- Удостоверяющий центр ПФР.
- Коммуникационная составляющая.

Похилько Е. Н.
ассистент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННОГО РОССИЙСКОГО ОБЩЕСТВА

В современном российском обществе информационная составляющая служит важным компонентом национальной безопасности. Понятие информационной безопасности не ограничено сугубо техническими параметрами. Так же в защите нуждается и общество, которому государство обязано предоставить информационно-психологическую безопасность. Информационно-психологическая безопасность в отношении личности состоит в защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства.[1]

Современное общество с легкостью оперирует такими понятиями как: "компьютерный вирус", "цветная революция", "информационная война","управляемый хаос", "социальная сеть", "кибератака" и пр.

Основным назначением информационного управления является воздействие на сознание людей, придание этому сознанию желательных качеств, соответствующих поставленной цели. Наиболее эффективным механизмом информационного управления являются СМИ и сеть Интернет. То есть те информационные источники, которые доступны и востребованы населением страны и которые привлекают, прежде всего, молодых людей. В зависимости от того, какие цели ставятся при информационном управлении, и пойдет процесс социализации в современном обществе. Таким образом, весь процесс социализации на современном этапе развития общества подвержен информационному управлению, и полярность этого управления зависит от усилий государства и общества в целом.[2]

За последние годы вектор большинства угроз национальной безопасности страны сдвинулся в сторону информационной сферы, в частности и военных угроз. И чтобы одержать победу над противником, необходимо иметь достаточно сильные информационные технологии и ресурсы. [3]

Интересы современного государства в информационной сфере заключаются в создании условий для развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества. Поскольку с развитием информационных технологий большая часть угроз и опасностей перемещается в информационную сферу, возникает необходимость развития и совершенствования не только самих технологий, но и нормативно-правовой базы, а также подходов к анализу и изучению угроз и приоритетов в информационной сфере, как одного из основных направлений обеспечения национальной безопасности страны.

Литература:

1. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.
2. Применение энтропии при моделировании процессов принятия решений в экономике / Королев О.Л., Куссый М.Ю., Сигал А.В. Монография / Под редакцией А.В. Сигала. - Симферополь, 2013. - 256 с.
3. Проблема манипуляции массовым сознанием как фактор дестабилизации информационной безопасности современного российского общества [Текст] / А. М. Руденко, Ю. А. Шестаков // Молодой ученый. — 2015. — №14. — С. 635-638.

УДК 519.866:331.5

Солдатов Максим Александрович
к.ф.-м.н., доцент
Макеева Галина Николаевна
магистрант
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ РЫНКА ТРУДА НА ОСНОВЕ УЧЕТА ТЕМПОВ РОСТА

Под прогнозированием понимают процесс составления оценок для будущих экономических событий. В литературе выделяют такой метод прогнозирования, как учет темпов роста. Рассмотрим данный метод на примере прогнозирования рынка труда. Методическая схема будет следующей:

1. Определение численности трудоспособного населения трудоспособного возраста на прогнозный период:

$$Ч_{пр} = Ч_{баз} + Ч_{баз} * Т_{срч}$$

, где:

$Ч_{пр}$ – численность населения трудоспособного возраста на прогнозируемый период;
$Ч_{баз}$ - численность населения трудоспособного возраста базового периода;
$Т_{срч}$ – среднегодовой темп прироста численности населения трудоспособного возраста

2. Определение предложения рабочей силы на прогнозный период:

$$П_{пр} = П_{баз} + П_{баз} * Т_{срп}, \text{ где}$$

$П_{пр}$ – предложение рабочей силы на прогнозируемый период,
$П_{баз}$ – рассчитанное предложение базового периода;
$Т_{срп}$ – среднегодовой темп прироста предложения рабочей силы;

3. Определение спроса рабочей силы на прогнозный период:

$$С_{пр} = С_{баз} + С_{баз} * Т_{срс}, \text{ где}$$

$С_{пр}$ – спрос рабочей силы на прогнозный период;
$С_{баз}$ – рассчитанный спрос базового периода;
$Т_{срс}$ – среднегодовой темп прироста спроса рабочей силы

4. Определение соотношения между спросом и предложением рабочей силы на рынке труда.

Прогнозирование каждого пункта базируется на анализе динамики за ряд предыдущих лет. При этом учитываются будущие изменения на необходимый период, с помощью моделирования всех составляющих. Также важным показателем для составления прогноза является динамика заработной платы. Ее уменьшение вызывает рост такого показателя, как: «самозанятость населения» или "черного рынка".

На основе модели было получены следующие расчеты при прогнозировании рынка труда Республики Крым на 2015год:

Показатели	Прогнозируемая численность	Прогнозируемое предложение	Прогнозируемый спрос
Результат (тыс. чел)	941,7	506,73	434,4

По результатам прогноза можно заключить, что проблемы безработицы острой формы не имеют, т.к. соотношение предложения и спроса составляет 85%. ($\frac{434,4}{506,73} * 100\%$). В базовом году соотношение предложения и спроса составило 93% (. Из вышесказанного, можно заключить, что уровень безработицы в прогнозируемом периоде увеличится, т.к. увеличению предложения нет соответствующего увеличения спроса на рабочую силу. Также наблюдается ситуация возможной утечки рабочей силы в «черный рынок», т.к. соотношение спроса и численности трудоспособного населения составляет 46 % ($\frac{434,4}{941,7} * 100\%$).

УДК 338

Черногорова К. А.
ассистент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРЕДУПРЕЖДЕНИЯ КРИЗИСОВ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Роль информационного аспекта в системе антикризисного управления тяжело переоценить, так как получение своевременной информации способно предотвратить наступление кризиса и существенно сэкономить ресурсы предприятия. Поэтому организации, направленные на упреждающее антикризисное управление, должны уделять процессам информатизации большое внимание. Информационное обеспечение превентивного управления в зависимости от специфики деятельности предприятия может существенно отличаться, различия в конфигурации обуславливаются разными информационными потребностями управления. В общем виде информационные потребности превентивного антикризисного управления детерминируются структурой его целей и задач. Главная цель упреждающего антикризисного управления – недопущение развития кризиса на предприятии, достигается решением следующих задач: мониторинг внешней и внутренней среды предприятия; распознавание угроз зарождения и развития кризиса; прогнозирование развития ситуации; диагностика кризиса на ранних этапах его развития; разработка рекомендаций по предотвращению кризиса и минимизации его последствий. В работах [1-2] была предложена информационно-аналитическая система предупреждения кризисных явлений на промышленных предприятиях (рис.1).

Основной задачей информационно-аналитической деятельности по предупреждению кризисов является поиск и отбор информационных ресурсов, необходимых для проведения исследований по прогнозированию кризисных ситуаций. Организацию работы с источниками информации целесообразно разбить на несколько этапов.

Первый этап – определение информационных потребностей. На данном этапе составляется перечень необходимой информации в разрезе пользователей.

Второй этап – определение источников информации. На этом этапе происходит формирование списка известных и доступных источников информации. Происходит оптимизация информации: исключаются дублирующая информация, источники с высокой стоимостью и низкой полезностью.

Третий этап – формирование системы коммуникаций, то есть осуществляется привязка источников информации к пользователям, происходит оптимизация информационных потоков.

Четвертый этап – формирование информационной политики. На данном этапе определяются виды и формы хранения информации, права доступа пользователей.

В результате работы системы информация претерпевает определенные видоизменения: происходит ее кодирование, выделение признаков, фильтрация, распознавание, осмысливание, выработка решения, формирование ответного действия.

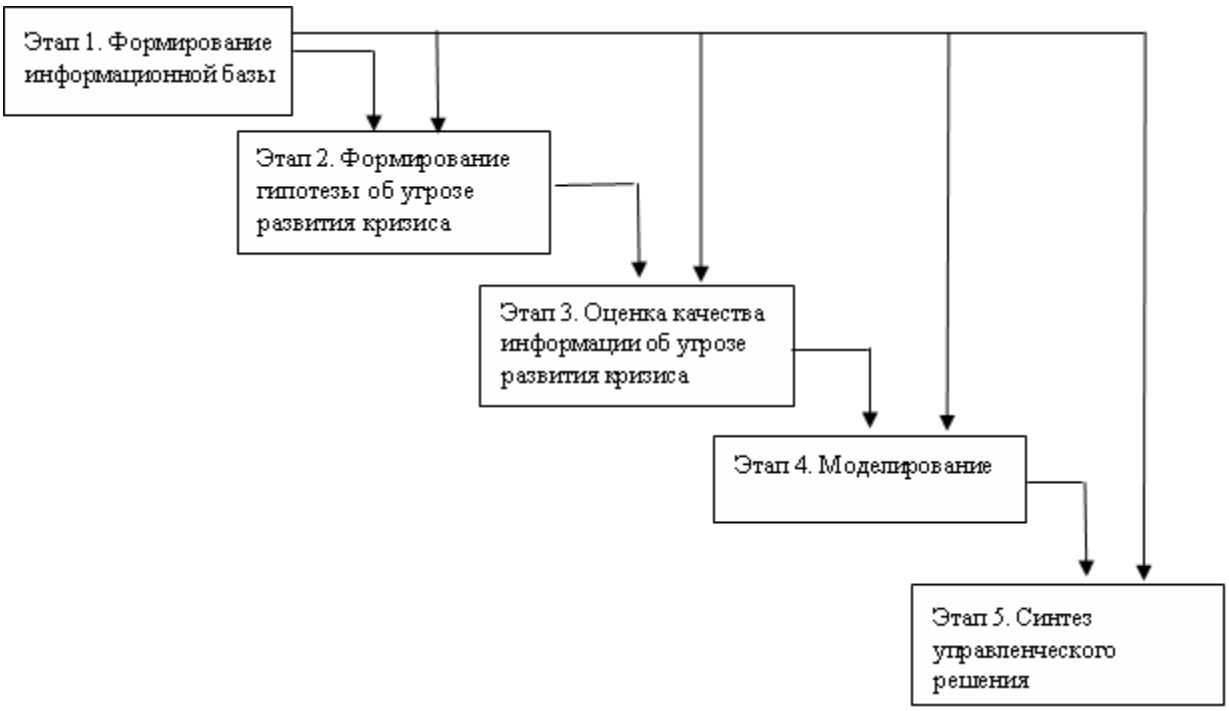


Рисунок 1. Основные этапы применения информационного подхода к предупреждению кризисных явлений.

Таким образом, информационный подход к предупреждению кризисов на промышленных предприятиях заключается, прежде всего, в уменьшении неопределенности в управленческих решениях за счет своевременного и максимального полного информационного обеспечения, а также в информационной поддержке прогнозирования кризисов.

Литература

1. Черногорова К.А. Информационный поход к предупреждению кризисных явлений на промышленных предприятиях // Вісник Хмельницького національного університету. – 2010, – № 5. Ч.2. Т.1. – С. 32 – 34.
2. Черногорова К.А. Предупреждение кризисных явлений на промышленных предприятиях // Матер. междунар. конф. «Актуальные проблемы и перспективы развития». - Симферополь-Гурзуф. – 2015. – С.176-177

УДК 657.63

Воробьев Юрий Николаевич
д.э.н., профессор
Чепорова Елена Валерьевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КОНФИДЕНЦИАЛЬНОСТЬ ИЛИ НАМЕРЕННОЕ ИСКАЖЕНИЕ УЧЕТНОЙ ИНФОРМАЦИИ ПРИ СЛИЯНИИ И ПОГЛОЩЕНИИ

В бухгалтерском учете проблема конфиденциальности обычно рассматривается с точки зрения деления бухгалтерского учета на финансовый, ориентированный на внешних пользователей, и управленческий, ориентированный на внутренних пользователей. Считается, что степень конфиденциальности для управленческого учета значительно выше, чем для финансового учета. Однако, на наш взгляд, проблема утечки информации несколько преувеличена. С одной стороны, учетные системы это не производственные технологии, а с другой стороны каждое предприятие достаточно уникально в рамках своей бизнес - модели для того, чтобы просто скопировать чужую систему. Это связано с тем, что основой конкурентных преимуществ может быть наличие стержневых компетенций, которые трудно скопировать.

Иногда за ссылкой на конфиденциальность скрывается попытка искажения или мошенничества с финансовой отчетностью.

В соответствие с общепринятыми стандартами финансовой отчетности, она должна правдиво и точно отражать финансовое положение, прибыльность и изменение в финансовом положении и не содержать существенных ошибок.

Аудит финансовой отчетности должен давать определенные гарантии, связанные с подтверждением правдивости информации.

Согласно Ассоциации сертифицированных экспертов мошенничества (ACFE) [2] «дерево мошенничества» включает в себя коррупцию, хищение активов и мошенничество с финансовой отчетностью.

Необходимость внешнего аудита, по сути, связана с информационной асимметрией между инсайдерами и аутсайдерами компании. Основная цель внешнего аудита финансовой отчетности является повышение доверия к раскрытым финансовым показателям для потенциальных инвесторов путем предоставления независимого аудита информации, представленной в финансовой отчетности. Следовательно, аудит высокого качества, скорее всего, уменьшает информационную асимметрию между информированными менеджерами и другими заинтересованными сторонами в компании. Тем не менее, роль внешнего аудитора была поставлена под сомнение после некоторых известных скандалов (например, Enron, WorldCom, Адельфия, Parmalat), приводящих к важным изменениям в законодательстве (например, акт Сарбейнса-Оксли в 2002 году), повышению ответственности аудиторских фирм и их независимости по отношению к своим клиентам. Недавний финансовый кризис привел к всплеску критики внешних аудиторов, поскольку все крупные аудиторские фирмы не в состоянии были обнаружить и сообщить о проблемах ипотечного кредитного рынка, которые привели к краху или попытке спасения многих важных финансовых компаний (например, Lehman Brothers, AIG, Fannie Mae и Freddie Mac).

Процедура слияния и поглощения (M&A) в этом контексте представляет особый интерес с точки зрения влияния качества аудита при наличии значительной информационной асимметрии между приобретаемой и целевой компаниями. Первая проблема информационной асимметрии касается стоимости целевой компании. Покупатели делают предложение для акционеров целевых компаний, основанные на их оценке стоимости компании (и ожидаемого повышения синергетической выгоды). Тем не менее, целевая компания лучше информирована о своей собственной стоимости, чем

покупающая компания. Один из способов уменьшить этот тип информационной асимметрии цены заключается в оплате за целевую компанию с учетом будущего повышения эффективности. Если покупатель предлагает акции, то стоимость предложения зависит от оценки сделки слияния на рынке, в результате чего происходит распределение рисков между целевой компанией и приобретателем. При оплате сделки денежными средствами, с другой стороны, покупатели берут на себя весь риск, даже если ожидаемое значение синергии, встроенное в премию приобретателя, не будут реализовано. Мы считаем, что необходимость в распределении рисков зависит от качества внешнего аудита финансовой отчетности. Высококачественный финансовый аудит, как ожидается, уменьшит неопределенность в финансовых показателях приобретаемой компании и, следовательно, ее значение для покупателя.

Вторая проблема информационной асимметрии связана с ценностью покупателя. Покупатели, имеющие личную информацию об их собственной ценности, могут попытаться использовать эту информацию, предлагая акции, если они переоценены. Это может объяснить, почему предложения акции, как правило, проявляется в низко прибыльных целевых фирмах. Аудит высокого качества смягчает информационную асимметрию и, следовательно, уменьшает влияние структуры капитала фирмы на поведение рынка.

Для большинства корпораций организационная трансформация является непрерывным процессом, который позволяет адаптироваться к постоянно изменяющейся глобальной бизнес-среде, привлекая достижения в технологии, науке, конкуренции, потребительском спросе и государственном регулировании. Наиболее распространенной формой изменения является реструктуризация (например, аутсорсинг, оффшоринг и т.д.). Наиболее сложной, драматичной и порождающей вызовы формой изменения является слияние и поглощение.

Согласно обзора Thomson Reuters [1] по слияниям и поглощениям 2014 г. был самым сложным годом для принятия решений по корпоративным сделкам начиная с 2007 года, при этом стоимость сделок по всему миру составили 3,5 трлн. дол. Некоторые из крупнейших объявленных сделок включали слияние Time Warner Cable с Comcast Corporation, оцениваемое в 71 млрд. дол., слияние Direct TV с AT & T за 67 млрд. дол. и слияние Allergan с Actavis plc за 58 млрд. дол.

Изменения являются неизбежными, но они подвергают компании значительным финансовым рискам и рискам мошенничества. В некоторых случаях, главные менеджеры используют реструктуризацию или слияние и поглощение в качестве инструмента для совершения мошенничества. С момента объявления компанией организационной трансформации до ее полного завершения система внутреннего контроля организации становиться слабой, поскольку она участвует в необычной деятельности в условиях значительной неопределенности, в том числе из-за страха потери рабочих мест и давления, связанного с требованием достижения запланированных финансовых результатов. Если организации не удается изменить свой стиль управления или быть не достаточно прозрачной, то это усугубляет риски мошенничества.

Исследования мошенничества показали, что давление усиливается в периоды перемен - давление является основным мотивом для совершения мошенничества. Исследования выявили «потребность удовлетворения внутренних или внешних ожиданий дохода» и «потребность совершенствования финансовой деятельности в связи с ожиданием справедливой доли или долгового финансирования», как наиболее часто цитируемых мотиваций при мошенничестве. Отчёт Ассоциации сертифицированных экспертов мошенничества (ACFE) 2014 года. по мошенничеству и злоупотреблениям отмечает, что в 26,4 процента случаев мошенничества в финансовой отчетности и 11 процентах фактов коррупции давление внутри организации был мотивом к совершению мошенничества [2, стр 61].

Реструктуризация может давить на высшее руководство с целей соблюдения или улучшения финансовых показателей. Они часто пытаются отразить такие финансовые

цели, как повышенная или устойчивая прибыльность, доходы, формирование положительного денежного потока и снижение затрат, сохраняя при этом высокий уровень качества и производительности. Сотрудники также могут быть объектом личного финансового давления из-за их чрезмерного долга в связи с жизнью не по средствам, игрой в азартные игры или проблем наркомании. Кроме того, давление может быть вызвано ухудшением общих экономических условий.

В условиях давления некоторые сотрудники будут искать способы использования возможностей для совершения мошенничества. Периоды изменения могут ослабить систему внутреннего контроля и сделать управленческий надзор и мониторинг систем внутреннего контроля неэффективными. Сотрудники могут выполнять контроль менее усердно, потому что им не хватает внимания, участия или лояльности к компании. Надзор может стать неэффективным, поскольку менеджеры планируют покинуть компанию. При пониженном контроле, в некоторых случаях, может возникнуть сговор сотрудников, чтобы переопределить контроль для личной выгоды.

Мошенники, как правило, способны рационализировать неправомерные действия независимо от организационных условий. Тем не менее, слияние или поглощение может спровоцировать сотрудников к совершению преступлений. Некоторые, возможно, объясняют это снижением лояльности при изменении своего положения или потерей рабочего места. Некоторые, возможно, считают, что изменение приводит к дискриминации и несправедливой практики. Другие могут сосредоточиться на правах, потому что они чувствуют себя недооцененными. В этой смеси давлений, расширении возможностей для совершения преступления и легкой рационализации мошенники могли бы найти себе выгодные условия для совершения мошенничества.

Следует отметить, что руководство и корпоративные советы, в конечном счете несут ответственность за эффективность системы внутреннего контроля и управления рисками мошенничества. В периоды перемен руководство должно продолжать поддерживать высокую целостность и задать тон в организации, чтобы напомнить сотрудникам, что основные ценности компании не изменились и что политика, в том числе по выявлению случаев мошенничества, остается в силе. К основным моментам в реорганизуемых организациях, на которые руководители должны обращать внимание, относятся:

- поддержание эффективного корпоративного управления и периодическое общение по ключевым контрольным мероприятиям с сотрудниками, чтобы напомнить им, что несмотря на переход, корпорация продолжает осуществлять внутренний контроль и требует его соблюдения;
- поддержание строгого контроля на уровне компаний;
- поддержание и развитие механизмов жесткого контроля в борьбе с мошенничеством, в том числе оценку риска внутреннего контроля и оценку рисков мошенничества;
- осуществление мониторинга деятельности, в том числе отчетов о внутреннем контроле, внутреннем аудите и разделении обязанностей.

И, самое главное, активно привлекать специалистов в области внутреннего контроля и борьбы с мошенничеством во время процесса изменений. Эти специалисты могут выполнить оценку риска и определить ведущие показатели ослабленного контроля.

Литература

1. Report to the nations on occupational fraud and a buse [Электронный ресурс]. – Режим доступа: http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

2. Mergers & acquisitions review reuters [Электронный ресурс]. – Режим доступа: http://www.dmi.thomsonreuters.com/dealsintelligence

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Усеинова Ленура Серверовна
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

УГРОЗЫ КИБЕРПРОСТРАНСТВА И ИХ ДИНАМИКА

В современном мире информационно-телекоммуникационные технологии все глубже проникают в нашу повседневную жизнь и этот процесс будет только ускоряться и усиливаться. Похоже, сегодня компьютеры и интернет повсюду - в сфере коммуникаций (электронная почта, мобильные телефоны), развлечений (цифровой кабель, мр3), транспорта (двигательные системы автомобилей, аэронавигация), торговли (онлайн-магазины, кредитные карты), медицины (оборудование, медицинская документация). По мнению ряда авторов [1], "В течение следующих 10 лет, количество интернет-пользователей возрастет до 4,75 млрд., объединяя более 91% населения развитых стран и около 69% населения стран с переходной экономикой". Допустимо утверждать, что угрозы киберпространству отличаются, по меньшей мере, тремя базовыми характеристиками: они распространены (затрагивают множество областей), разнообразны и внедряются в систему. Первая характеристика отражает тот факт, что характер потенциальной стратегической угрозы распространяется на любой из элементов киберпространства. Вторая — потенциальная угроза исходит от операционных систем, программного обеспечения и самого компьютерного оборудования (и, следовательно, никогда не может быть полностью искоренена). Третья характеристика означает, что киберпространство включает в себя не только адекватных национальных пользователей, но и различные террористические организации, преступные группировки, в том числе хакеров.

Существует, также, и несколько специфических характеристик, отличающих угрозы в киберпространстве и в реальном мире. К ним можно отнести:

1. Глобальный характер киберпространства сталкивается с действиями государственных и национальных институтов, придерживающихся разных правовых и культурных интересов и целей;

2. Мир стал зависимым от киберпространства для обеспечения связи, контроля физического мира и даже для обеспечения национальной безопасности;

3. Локализация производства программного и аппаратного обеспечения функционирования киберпространства делают практически невозможным реальный контроль качества и безопасности их использования;

4. Абсолютное большинство пользователей аппаратного и программного обеспечения киберпространства не способны реально контролировать используемые ими элементы глобального киберпространства, и, следовательно, происходит постепенная концентрация власти;

5. Из-за концентрации власти становится вынужденной согласованность позиций для предотвращения почти любых угроз в киберпространстве;

6. Каждый виток развития информационно-коммуникационных технологий порождает новые угрозы киберпространству;

7. Не все ресурсы киберпространства подконтрольны и сохраняется анонимность авторов угроз;

В общем рейтинге угроз, послуживших причиной утечки ценных данных в компаниях, лидируют атаки с использованием вредоносного программного обеспечения (24%). На втором месте – незакрытые уязвимости (14%), а на третьем – случайная утечка данных, спровоцированная сотрудниками (8%). Кроме того, представляет несомненный интерес и тот факт, что “для среднего и малого бизнеса перечисленные выше основные

угрозы представляют бóльшую опасность (в среднем показатель выше на 5%)". "Вирусы, черви, шпионские программы и др. вредоносное ПО приводят к потерям до 40% данных" [2]. При этом 82% специалистов по ИТ-безопасности ожидают роста инцидентов в киберпространстве и лишь 14% сообщают, что "их элементы киберпространства реализовали планы мероприятий по обеспечению кибербезопасности" [3].

В результате проведения данного исследования можно отметить, что абсолютное большинство исследований обеспечения кибербезопасности ориентировано в настоящее время на защиту технической (технологической) составляющей киберпространства. Решение проблем обеспечения кибербезопасности должно учитывать не только технический, но и гуманитарный, социальный и духовный факторы, так как онтологическая проблематика феномена киберпространства (помимо систем компьютерной виртуальной реальности и сфер их применения) включает в себя не только психологическую виртуальную реальность (рассматриваемую как отражение психикой процессов, происходящих в самой же психике, то есть самообраз), но и социально-философские проблемы сетевой коммуникации, а также экзистенциально-психологические аспекты сетевой коммуникации и специфику виртуальной идентичности.

Список использованных источников:

1. Burt D. Cyberspace 2025 Today's Decisions, Tomorrow's Terrain. / D. Burt, A. Kleiner, J. P. Nicholas, K Sullivan. [Электронный ресурс]. — Режим доступа: http://www.cyberspace2025.com

2. Информационная безопасность бизнеса. Исследование текущих тенденций в области информационной безопасности бизнеса за 3 квартал 2015 г. // Лаборатория Касперского» совместно с международной аналитической компанией B2B International. ЗАО «Лаборатория Касперского», 2015.

3. Security Services Research. Essential reports on today's security landscape. Report "2015 Cost of Data Breach Study". [Электронный ресурс]. — Режим доступа: http://www-03.ibm.com/security/data-breach/?cm_mc_uid=93180806712214394653672&cm_mc_sid_50200000=1439484820

УДК 004.057.2

Акинина Людмила Николаевна
старший преподаватель
Зенцов Александр Сергеевич
студент 2 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПОРЯДОК РАЗРАБОТКИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Прежде всего, политика необходима для того, чтобы донести до бизнеса цели и задачи информационной безопасности (ИБ) компании. Бизнес должен понимать, что специалист по защите данных это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а следовательно в повышении прибыльности компании.

Политика ИБ необходима для обоснования введения защитных мер в компании. Политика должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.).

Любая защитная мера является компромиссом между снижением рисков и удобством работы пользователя, потому сотруднику IT-подразделения компании необходимо предложить модель процесса, в которой эти риски снижены в какой-то мере, удовлетворительной для бизнеса.

При этом любое применение любых защитных мер, касающихся взаимодействия пользователя с информационной системой компании всегда вызывает отрицательную реакцию пользователя. Практика показывает равнодушное отношение пользователя в отношении рисков, несмотря на пропаганду пагубного влияния хакерских атак, ответственности пользователя за допущение порети данных и т.д.

Однако наличие в компании политики позволяет вводить данную меру для исполнения требований политики информационной безопасности компании, которая утверждена высшим административным органом компании

При разработке политики следует учитывать о два основных момента:

1. Целевая аудитория политики ИБ - конечные пользователи и топ-менеджмент компании, которые не понимают сложных технических выражений, однако должны быть ознакомлены с положениями политики;

2. Четко обозначенные только целей ИБ, методы их достижения и ответственность. Никаких технических подробностей, если они требуют специфических знаний и используются в качестве материалов для инструкций и регламентов.

Конечный документ должен удовлетворять следующим требованиям:

- лаконичность (большой объем документа отпугнет любого пользователя);
- доступность (конечный пользователь должен понимать, что написано в политике).

УДК 004.451.25

Герасимова Светлана Васильевна
д.э.н., профессор
Голубев Александр Андреевич
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ СИСТЕМ SAP ERP В ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

Для достижения стратегических целей компании и реализации программ развития необходимо инвестировать, и соответственно, нужно обеспечить качественное управление инвестиционной деятельностью.

Несколькими из этапов управления инвестиционной деятельности являются: выбор инвестиционной стратегии предприятия и постинвестиционный мониторинг с оценкой результатов инвестиционной деятельности. На данных этапах автоматизация вышеизложенных процессов будет играть важную роль в экономии временных, человеческих и экономических ресурсов. Для автоматизации инвестиционной деятельности целесообразно использовать систему SAP.

Система управления ресурсами предприятия SAP ERP обеспечивает автоматизацию процессов управления проектами и значительно облегчает управление портфелями проектов.

Планирование ресурсов предприятия при помощи ERP-системы обеспечивает полный функционал, необходимый для осуществления самообслуживания, предоставления информационных услуг, проведения аналитики, управления финансами, персоналом, операциями и обслуживанием клиентов, а также прогнозирования целесообразности инвестиций. Решение включает в себя четыре области применения, функциональные возможности которых формируют надежную основу для реализации эффективных бизнес-процессов.

Кроме того, SAP ERP предоставляет инструменты для выполнения задач системного администрирования, таких как управление пользователями, централизованное управление данными и управление Web-сервисов [1].

Система управления ресурсами предприятия SAP ERP обладает уникальными свойствами и имеет ряд неоспоримых преимуществ, которые аргументируют целесообразность и результативность ее использования в инвестиционной деятельности современных предприятий.

В частности, к основным свойствам SAP в инвестиционных проектах относят:

- поддержку модели жизненного цикла инвестиционного проекта;
- планирование фаз и точек принятия решения;
- гибкое определение условий смены фазы;
- внесение в систему решения о завершении фазы;
- поддержка различных жизненных циклов, в зависимости от типа проекта;
- автоматизацию согласованного процесса управления изменениями на уровне инвестиционной программы.

В качестве основных преимуществ ERP-системы называют следующие:

- включает в себя все необходимые для жизнедеятельности предприятия области функционирования, поэтому он может заменить большинство используемых в настоящее время систем;
- содержит опыт лучших компаний в отрасли, выраженный в готовых процессах и документации;
- позволяет интегрировать новое решение с существующей системой, которая сокращает инвестиции в текущем решении.

При необходимости, она может быть использована в сочетании со сторонними программными решениями. В зависимости от цели внедрения ERP-решения SAP могут применяться разными пользователями, нуждающимися в информации, которая хранится в системе. Чаще всего, в качестве таких пользователей выступают сотрудники коммерческого отдела, IT, маркетинга, бухгалтерского учета и других.

Системы управления инвестиционной деятельности позволяют обеспечить информационную поддержку жизненного цикла проектов по инвестициям, эффективное планирование и управление ходом работ, в соответствии с заранее определенными нормами и требованиями.

Для того, чтобы начать работу над проектом внедрения программной системы, необходимо сформулировать цели внедрения, подготовить стратегию внедрения, масштабировать и оценить предстоящий проект. Авторы предлагают руководителю проекта вначале сгенерировать свои идеи, структурировать и визуально их представить при помощи интеллект-карты (карты ума, ментальной карты). Интеллект-карта - это эффективный инструмент структурирования и анализа информации, позволяющий ускорить разработку бизнес-проектов [2].

Внедрение ERP-системы позволяет избежать институциональной стандартизации, информационной асимметрии, способствует развитию сотрудничества и взаимодействия как внутри организации, так и между ними.

Сегодня, согласно распространенному мнению экспертов, одним из самых передовых решений в области управления активами является SAP AG, которое было разработано немецкой компанией. Следует отметить, что процесс управления инвестициями и строительством – это деятельность, связанная с использованием активов предприятия и принятием решений по техническому обслуживанию и ремонту.

Для управления инвестиционной деятельностью с помощью SAP широко используются специальные компоненты: модули PS (Project System) и PPM (Portfolio and Project Management). PS глубоко интегрирован с другими модулями ERP- системы, такими как FI, CO, MM, PM [3].

Отечественным лидером отрасли, безусловно, является компания 1С. Все остальные разработки отечественных компаний не могут конкурировать с западными вендорами. Основное различие в масштабах. Западные решения идеально подходят для крупных международных компаний, у которых ежедневно происходит множество транзакций в разных валютах, разных странах, разных часовых поясах и т.д. Такие системы могут поддерживать одновременную работу нескольких тысяч сотрудников, хранить значительные объемы данных. Технически такой масштаб 1С не может поддерживать, но она вполне применима для решения локальных задач [4].

Одной из основных практических проблем, возникающих при внедрении ERP-систем, подсистем, управления производством и особенно планирования, является низкое качество или отсутствие нормативно-справочной информации, конструкторской и технологической документации.

Необходимо создать условия для полноценного планирования ERP-системы. Есть реальная возможность провести экономический анализ материалов и комплектующих изделий с целью оптимизации их использования и выявления возможностей замены. И одна из этих замен должна быть определена как постоянная, а другая - как приемлемая. Это позволит оптимизировать ассортимент закупаемой продукции для предотвращения замещения в производственном процессе. В результате сокращается общий список номенклатуры.

Как известно, при использовании правильной ERP-системы применяются такие механизмы для планирования и учета, как "набор-комплект" и "побочный продукт".

Механизм «набор-комплект» обеспечивает возможность описания ситуации, в которой из одной заготовки получают заранее известное количество изделий (не обязательно одинаковых). Механизм «сопродукт» обеспечивает возможность более точного планирования расхода материалов. В итоге, на производстве практически устраняется необходимость бесконтрольных замен материалов. При использовании

ERP-системы появляется возможность автоматического учета и дальнейшего планирования деловых отходов [5].

Таким образом, интеграция отобранных программных продуктов обеспечивает необходимую функциональность и является хорошей альтернативой более дорогим и сложным в использовании системы управления проектами. Практическая ценность заключается в экономии времени руководителя проекта и избавления его от рутинной работы.

Благодаря системе SAP обеспечивается необходимое построение структуры инвестиционной программы, в которой могут быть соединены показатели отдельных проектов и показатели инвестиционных программ и портфелей. Также возможно совместное использование нескольких альтернативных представлений инвестиционной программы.

Данная система поддерживает процесс финансового планирования и контроля реализации проектов, инвестиционных программ, портфелей проектов. Обеспечивает гибкое определение состава финансовых показателей, планирование и учет натуральных показателей проекта.

Одной из важнейших ролей SAP в организации инвестиционной деятельности предприятия является автоматизация процессов ранжирования проектов, который, как правило, осуществляется при наличии нескольких проектов.

Перечень использованных источников:

1. Система SAP ERP, комплекс решений SAP [Электронный ресурс]. - Режим доступа: http://www.norbit.ru/products/197.html

2. Мюллер Х. Составление ментальных карт. Метод генерации и структурирования идей / Х. Мюллер. -М., Омега-Л, 2007. - 356 с.

3. Автоматизация инвестиционной деятельности на энергетическом предприятии [Электронный ресурс]. - Режим доступа: http://www.iemag.ru/analitics/detail.php?ID=23424

4. Внедрение ERP-систем. Актуальность и тенденции [Электронный ресурс]. - Режим доступа: http://www.intalev.ua/library/articles/article.php?ID=5072&sphrase_id=918

5. Внедрение системы управления класса ERP [Электронный ресурс]. - Режим доступа: http://www.intalev.ua/library/articles/article.php?ID=5054&sphrase_id=918

УДК 338.364.2

Герасимова Светлана Васильевна
д.э.н., профессор
Федоров Евгений Александрович
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ АВТОМАТИЗАЦИИ ПРОЦЕССА ФОРМИРОВАНИЯ ОТЧЕТНОСТИ ПРЕДПРИЯТИЯ

В ходе формирования абсолютно любой отчетности могут возникнуть проблемы, которые негативно повлияют на эффективность всей системы управления предприятием. Эти проблемы неизбежны, но их можно нейтрализовать или избежать при условии правильной организации автоматизации отчетности предприятия.

В функционировании любого предприятия неизбежны процессы образования разного вида отчетности для внутренних (менеджеры) и внешних (акционеры, государство) пользователей.

Для крупных предприятий характерны низкая формализация, высокая трудоемкость, малая оперативность и, зачастую, недостоверность предоставляемой отчетной информации [2]. Приведем более подробные характеристики обозначенных выше проблем.

Любое структурное подразделение, функционирующее при крупном предприятии, образует особый пакет подотчетности. Стоит заметить, показатели в отчетах разных

подразделений могут пересекаться, однако, данный процесс никем не контролируется. Руководители могут сменяться, при этом состав отчётности каждого подразделения пересматривается. Это приводит к возникновению новых форм, но никак не отменит уже существовавшие. Как итог, отчетность предприятия становится излишней, при этом повышается трудоемкость процессов ее формирования, но потребители информации от этого практически ничего не выигрывают.

Что касается сотрудников, то далеко не каждый сотрудник предприятия, который предоставляет отчет, имеет интерес, чтобы данный процесс получения информации о сведениях был абсолютно «прозрачен». Такая чрезмерная открытость усиливает контроль руководства над сотрудниками, поэтому не приветствуется факт того, что сам процесс формирования отчетности непосредственно на местах будет формальным.

Если на предприятии формализация процесса формирования отчетности низка, то данный факт побуждает к умышленному искажению какой-либо информации. При повышении трудоемкости снижается оперативность. Это связанно с тем, что штат сотрудников ограничен и сохранились прежние способы и методы формирования подотчетных руководству документов.

Касаемо самого процесса непосредственной доставки информационных сведений (отчетов) лицу, которое принимает решение (конечному пользователю отчета, начальству), он вполне может иметь несколько ступеней, звеньев. Каждое звено подвержено задержкам и искажениям информации.

Реорганизация процессов формирования отчетности возможна с применением механизма их автоматизации. Общеизвестно, что автоматизация, являясь одним из направлений научно-технического прогресса, использует саморегулирующие технические средства и математические методы с целью освобождения человека от участия в процессах получения, преобразования, передачи и использования энергии, материалов, изделий или информации, либо существенного уменьшения степени этого участия или трудоёмкости выполняемых операций.

Автоматизированная форма бухгалтерского учета, основанная на использовании электронно-вычислительной техники, представляет собой комплексную систему автоматизации учетного процесса, начиная со сбора первичных данных до получения бухгалтерской отчетности. В настоящее время на российском рынке программных продуктов сегмент бухгалтерских программ наиболее объемный и составляет около 500 различных программ. Наиболее популярными являются: «1С: Бухгалтерия», «БЭСТ», «Турбо-бухгалтер», «Парус», «Инфо-бухгалтер» [6].

Как свидетельствует практика, автоматизация процесса формирования отчетности позволяет получить следующие преимущества:

- возможность одновременно с созданием документа формировать типовые корреспонденции счетов, что значительно сокращает учетный процесс и позволяет своевременно создавать необходимые отчеты;
- повышение аналитичности расчетов за счет возможности добавления к отдельным бухгалтерским счетам дополнительных признаков аналитики, в результате чего на этих счетах, кроме учетных данных, могут отражаться плановые или нормативные показатели;
- ускорение процесса калькулирования за счет увеличения скорости выполнения арифметических операций;
- повышение аналитичности информации калькуляционных листов благодаря одновременному использованию большого перечня статей;
- ускорение процесса и неограниченная частота формирования бухгалтерской отчетности, а также повышение достоверности и аналитичности отчетности.

В условиях автоматизации значительное совершенствование техники учета характеризуется расширением аналитических и контрольных функций на основе методологического единства данных первичного учета и основных учетных регистров. Определенный набор учетных функций, заложенный в алгоритмы программы, позволяет

автоматизировать элементы метода бухгалтерского учета, а именно документацию, ведение счетов, двойную запись, оценку, калькуляцию и др. [5, с. 70].

Автоматизированные программные решения развиваются в направлении максимизации функциональности и снижения трудоемкости для конечных пользователей. Использование методов математической статистики и эконометрики, в условиях конкурентной борьбы привело к появлению финансово-аналитических программ, позволяющих оценить финансовое состояние [3, с. 6].

Однако автоматизация процесса формирования отчетности сопряжена с рядом проблем. Основная проблема, связанная с автоматизацией деятельности на предприятиях, по мнению специалистов, заключается в том, что источник информации по показателю для автоматизации отчета может быть не определен. В качестве основных решений обозначенной проблемы практики предлагают более точное определение источника данных, расширение функционирования информационных систем предприятия, отказ от процесса автоматизации или формирования отчета в прежнем виде. Перечисленные действия, прежде всего, направлены на идентификацию необходимых источников и определение требований по изменению функциональности информационных систем предприятия [2].

Конкретные проблемы, с которыми сталкиваются предприятия, во многом определяются особенностями используемого пакета программного обеспечения. Некоторые предприятия могут использовать несложные автоматизированные системы формирования отчетности, например, на основе продуктов Microsoft Excel. В данном случае возникают проблемы высокой трудоемкости и низкой функциональности подобных решений [4, с. 57].

Для наиболее часто используемой платформы компании «1С» свойственны такие проблемы, как изолированность от глобальной сети (с целью обеспечения достаточного уровня безопасности), необходимость приобретения дополнительного количества ключей [1, с. 4]. Исходя из этих проблем, предприятия разрабатывают собственные программные решения на платформе Net Framework. Крупные предприятия зачастую используют автоматизированные системы собственной разработки, что позволяет максимально приблизить функциональность к запросам предприятия, однако проблемой является стоимость разработки и содержания таких систем, как правило, она достаточно существенна.

Таким образом, использование предприятиями автоматизированных систем формирования отчетности позволяет достичь некоторых преимуществ и разрешить ряд серьезных проблем, таких как высокая трудоемкость и возможность занесения в отчетность недостоверных данных. В свою очередь, автоматизации процесса формирования отчетности также свойственны некоторые проблемы: искажение информации, низкая функциональность, высокая стоимость. Для разрешения этих проблем необходим комплексный подход, учитывающий потребности предприятия и его возможности. Также при создании или приобретении автоматизированной системы формирования отчетности следует учитывать перспективы роста предприятия и предусмотреть резервы для этого роста.

Список литературы:

1. Воронина В. В. Технологии автоматизации бизнес-процессов предприятий : учеб. пособие / В. В. Воронина. – Ульяновск : УлГТУ, 2013. – 204 с.

2. Гилев А. Автоматизация отчетности предприятий / А. Гилев // Директор информационной службы [Электронный ресурс]. – Настольный журнал ИТ-руководителя. – 2006. – № 3. – Режим доступа : http://www.osp.ru/cio/2006/03/379915/

3. Гусева Е. С. Роль информационных технологий в процессе формирования финансовой информации интегрированной отчетности / Е. С. Гусева, Д. В. Круглов // Современные проблемы науки и образования: электр. науч. журнал – 2014. – № 6.

4. Пикалов И. Ю. Достоинства и недостатки автоматизации процесса составления корпоративной отчётности и её анализа / И. Ю. Пикалов // Auditorium: электр. науч. журнал Курского государственного университета. – 2015. – № 1 (5). – С. 56-60.

5. Сафина З. З. Автоматизация формирования отчетности в соответствии с МСФО в современных условиях / З. З. Сафина // Журнал «Перспективы развития информационных технологий». – 2014. – Вып.

21. – С. 69-73.
6. Хайбуллина И. В. Автоматизация бухгалтерского учета: проблемы и перспективы / И. В. Хайбуллина, М. Е. Куланина, Л. С. Бахчеева // Экономика и менеджмент инновационных технологий [Электронный ресурс]. – Электронный научно-практический журнал. – 2015. – № 4. – Режим доступа : http://ekonomika.snauka.ru/2015/04/8539

УДК 004.056.53

Гончарова Оксана Николаевна
д.п.н., профессор
Никифоров Сергей Владимирович
магистрант
Таврическая академия, факультет математики и информатики
КФУ имени В.И. Вернадского
Республика Крым, Россия

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКИХ СИСТЕМАХ

В России, помимо крупнейших игроков банковского сектора, существует множество небольших банков, которые, в силу финансовых ограничений, не могут позволить себе вкладывать значительные суммы в информационную безопасность. Тем не менее, безопасность информационных систем банков любого масштаба должна строиться с использованием ряда основных принципов. Банковская сеть, как сеть любого предприятия или организации, содержит в своем составе вполне стандартный набор объектов: рабочие станции сотрудников, инфраструктурные и специализированные серверы, сетевые шлюзы. С развитием мобильности к этому набору все чаще добавляются ноутбуки, смартфоны и планшеты, с которых осуществляется доступ сотрудников к банковской информационной системе. Специфика банков состоит в том, что к этому набору добавляются банкоматы и платежные терминалы. Задача защиты информации, хотя и близка по схеме и используемым средствам к задачам, решаемым для обычной организации, также должна иметь ярко выраженную банковскую специфику. Необходимо:

1) Обеспечить надежную и безопасную работу АБС (автоматизированной банковской системы).

2) Обеспечить безопасный доступ сотрудников и клиентов к банковской системе в территориально распределенной сети.

3) Обеспечить доступ сотрудников к внешним информационным сетям (Интернету).

4) Обеспечить защиту банкоматов и терминалов.

5) Иметь возможность контроля всех процессов в системе и своевременного обнаружения любых нарушений.

Все эти задачи необходимо решать комплексно, начиная с архитектуры банковской сети. Хорошей и достаточно распространенной практикой является создание нескольких изолированных сетей с минимальным количеством точек взаимодействия (шлюзов) с применением самых современных средств защиты. Что касается специализированного ПО, то по-прежнему основой систем информационной безопасности являются антивирусные программы. За несколько последних лет они эволюционировали от «просто антивирусов» до комплексных систем защиты контроля рабочих станций. Безопасность данных при хранении требует использования средств шифрования, которые смогут работать либо на уровне хранилищ данных, либо на уровне отдельных компонентов системы, например, таблиц баз данных. Безопасность банкоматов и платежных терминалов должна обеспечиваться с использованием традиционных средств — антивирусной защиты. Но в то же время специфика таких устройств требует применения дополнительных средств защиты, включая создание «замкнутой программно-аппаратной среды», полностью исключающей установку любого стороннего ПО и подключение внешних устройств. Подводя итог, можно сделать

главный вывод. Информационные системы банков имеют ярко выраженную специфику, но для защиты информации во многом пригодны те же методы и средства, что используются в «обычной» жизни. Главное — подходить к построению системы безопасности максимально ответственно, учитывая все узкие моменты, так как цена ошибки в данном случае очень высока.

УДК 32.019.51

Гончарова О. Н.
д.п.н., профессор
Самсонов К.
магистрант
Таврическая академия, факультет математики и информатики
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МЕТОДИКА ПОСТРОЕНИЯ КОРПОРАТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Главная цель любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации, обеспечении нормальной производственной деятельности всех подразделений объекта.

При построении корпоративной системы защиты информации (КСЗИ) предлагаем использовать следующую модель построения КСЗИ (рис. 1).

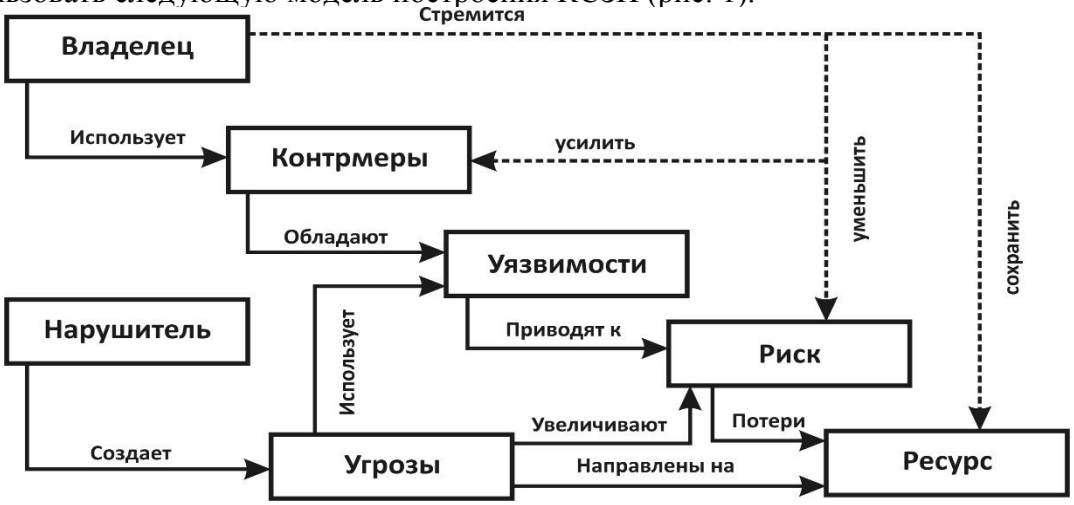


Рис.1. Модель построения корпоративной системы защиты информации

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности.

Согласно предложенной модели, при построении КСЗИ следует

- максимально полно определить потенциальные угрозы методом экспертных оценок;
- изучить все возможные уязвимости системы, причем не только программные и аппаратные, но и с учетом человеческого фактора;
- на основе понимания угроз и уязвимостей следует рассчитать возможные риски, а также разработать направления их уменьшения;
- составить план применения контрмер при наиболее вероятных вторжениях или

других внештатных ситуациях.

Применение предложенной схемы разработки и внедрения КСЗИ позволит путем усиления контрмер уменьшать риски и в результате сохранить финансовые, трудовые и информационные ресурсы предприятия.

Королёв Олег Леонидович
к.э.н., доцент
Бердников Даниил Дмитриевич
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

СТАНДАРТЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Стандарты безопасности информационных систем – это рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня информационной безопасности и установлены требования к безопасным информационным системам. [1]

Благодаря стандартам информационной безопасности производители и эксперты обоснованно определяют наборы требований к информационным продуктам и декларируют их возможность, подтверждают ценность продуктов путём сертификации на соответствие стандартам информационной безопасности, получают ценную техническую и иную информацию. Потребители обоснованно выбирают информационные продукты, более чётко формулируют требования к ним, имеют возможность построить гарантированно качественную систему ИБ. [3]

Стандарты безопасности информационных систем можно классифицировать: по области регламентации, по территории распространения, по обязательности выполнения, по доступности.

Существуют российские стандарты информационной безопасности (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 51275 и др.), причем Федеральный закон №184-ФЗ «О техническом регулировании» декларирует принцип «применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения». [2]

Необходимость следования некоторым стандартам информационной безопасности закреплена законодательно. Однако и добровольное выполнение стандартов очень полезно и эффективно, поскольку в них описаны наиболее качественные и опробованные методики и решения.

Список литературы

1. Стандарты информационной безопасности. [Электронный ресурс]. — Режим доступа: http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html
2. Федорова Я.В., Попова Л.К. Методические подходы к анализу информационной безопасности [Электронный ресурс]. — Режим доступа: http://studopedia.org/8-118391.html
3. Модели и информационные системы современной экономики. Монография / Апатова Н.В., Бойченко О.В., Герасимова С.В., Пенькова И.В., Сигал А.В., Дюличева Ю.Ю., Иванов С.В., Королев О.Л., Круликовский А.П., Попов В.Б., Рыбников М.С., Солдатов М.А., Акинина Л.Н., Бакуменко М.А. // Под редакцией Н.В. Апатовой. - Симферополь, 2015. – 520 с.

УДК 338.45 : 004.35

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Пушкарева Елена Викторовна
старший преподаватель
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия
Круликовский Сергей Анатольевич
Начальник группы разработки ПО ООО "ТРИЭС СОЛЮШНЗ",
г.Киев, Украина

ШИФРОВАНИЕ ОПЕРАТИВНЫХ ДАННЫХ В УПРАВЛЯЮЩЕЙ СИСТЕМЕ НА ПЛАТФОРМЕ «1-С ПРЕДПРИЯТИЕ»

Проблема несанкционированного доступа к корпоративной информации является значимым источником разнообразных коммерческих рисков для любого бизнеса. Количество правонарушений в области компьютерных технологий хранения корпоративных данных постоянно увеличивается, данные можно и скопировать и незаметно видоизменить или даже уничтожить.

Специалисты в области информационной безопасности США оценили, что ущерб от компьютерных преступлений увеличивается на 35 процентов в год. Причем финансовый ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, тогда как при ограблении банка - всего лишь 19 тысяч долларов.

Аналитический Центр компании InfoWatch в практическом исследовании уровня защиты корпоративной информации в промышленности отметил явное преобладание трех типов угроз – утечка ноу-хау, нелояльное поведение сотрудников (сговоры с целью получения отката, шпионаж, саботаж) и злоупотребление доступом. Данные проблемы стоят перед руководством любого по размерам предприятии.

Корпоративные системы управления средних и малых предприятий России строятся в основном на платформе «1С-Предприятие». Часто средства информационной защиты успешно функционирующих в крупных организациях, не смогут найти применения для среднего и малого бизнеса,

Для предприятий среднего и малого бизнеса, где, в качестве управляющей системы, используется конфигурация на платформе «1С Предприятие», предлагается использовать в качестве движка шифрования бесплатную компоненту Microsoft – Capicom.dll или аналогичные. Данная компонента позволяет шифровать любые строковые данные с заданным паролем. В корпоративную систему управления предприятием, представляющую собой конфигурацию на платформе «1С Предприятие» добавляется общий модуль управления шифрованием, а для всех значимых полей документов, подлежащих шифрованию, устанавливается «двойная типизация данных»: добавляется тип «Строка». Для шифрования значимых числовых данных добавляется поле «Множитель».

Общий модуль управления шифрованием выполняет следующие функции:

1. Контролируется наличие или отсутствие ключа.
2. Производится преобразование данных и шифрование с использованием криптостойкого пароля.
3. Расшифровка данных. Процедура обратная шифрованию.

В базу данных записываются только зашифрованные данные, расшифрованные данные предназначены только для вывода на формы.

Для построения отчетов по зашифрованным данным используются предварительная расшифровка.

Данная модель организации информационной безопасности в корпоративных системах управления позволяет ограничить доступ к корпоративной информации полностью, без разделения по правам пользователей. Доступ к данным должен

предоставляться любому пользователю, который имеет «Ключ» (аппаратная часть) и знает «Пароль» (программная часть).

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Семенова Юлия Андреевна
старший преподаватель
Бутенко Татьяна Владимировна
магистрант
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

Современные предприятия используют Интернет как основной инструмент для развития деловой активности и охвата рынка, что, в конечном счете, приводит к финансовым выгодам. Наряду с этими преимуществами появляются различные угрозы безопасности важной корпоративной информации.

В современном мире информационная безопасность предприятия играет очень важную, а зачастую и первостепенную роль. Традиционно, безопасность рассматривалась как государственная или политическая функция, но тенденция современных технологий в 21 веке свидетельствует, что традиционные представления о защите информации, данных и активов в пределах предприятия необходимо пересмотреть. Причины этого в участившихся хакерских атаках. Мотивы для атаки могут быть самыми разными от взлома с целью наживы, что зачастую является основным, до мести обиженных экс-сотрудников. В результате нарушается безопасность управления банковских баз данных, происходит кража ценной корпоративной информации. И, что немаловажно, необязательно быть специалистом в программировании, чтобы иметь возможность создать угрозу нарушения безопасности в Интернете, для этого есть много инструментов онлайн, которые доступны любому пользователю. Это, наверное, самая актуальная проблема, вызывающая озабоченность по поводу безопасности для предприятия в современную эпоху.

Для стабильной работы на каждом предприятии должна быть разработана и утверждена политика безопасности, в том числе и информационной, которая является составной частью общей политики безопасности. Основами информационной безопасности являются: конфиденциальность, целостность и доступность, вот три основных основополагающих принципа всех систем безопасности.

Конфиденциальность должна быть сохранена, независимо от того в каком формате хранится информация. Строгий контроль доступа, информационная подготовка пользователя и шифрование данных являются контрмерами, которые помогают обеспечить безопасность корпоративной информации от нарушения конфиденциальности.

Все инфраструктуры информационных систем, как правило, должны работать совместно для обеспечения целостности данных и информации в корпоративной операционной среде. Жесткий контроль доступа, системы обнаружения вторжений могут смягчить эти угрозы. Пользователи системы могут также ошибочно ввести неверные исходные данные в информационную корпоративную систему.

Приложения должны быть оснащены возможностями для проверки входных данных на наличие ошибок. Кроме того, должны быть даны специальные разрешения и полномочия специалисту соответствующей квалификации на ознакомление, и тем более, на изменение корпоративных данных, чтобы убедиться, что эти изменения не были случайными или преднамеренными.

Восстановление системы после сбоев так же является важным фактором, когда речь идет о целостности и доступности информации. Восстановление корпоративных данных должно быть проведено таким образом, чтобы не повлиять негативно на саму информацию. Доступность гарантирует, что доступ к данным осуществляется уполномоченными лицами, что обеспечивает надежность и эффективность работы корпоративной информационной системы. Своевременная установка исправлений для операционных и пользовательских систем, правильная конфигурация маршрутизаторов, применение рабочей станции управления конфигурациями и использование брандмауэра – это только некоторые из способов предотвращения атак, направленных на доступность системы.

Эффект от атаки может иметь очень разрушительные последствия для бизнеса. Необходимо иметь в штате предприятия экспертов, которые будучи хорошо подготовленными в области информационной безопасности, смогут избежать ситуаций, наносящих вред предприятию. Персонал предприятия должен быть обучен для повышения уровня осведомленности и бдительности. К сожалению, все чаще руководители предприятия сокращают расходы и повышают рентабельность с помощью аутсорсинга, передавая важнейшие задачи управления предприятием сторонним организациям, повышается тем самым степень риска для бизнеса.

УДК 004.58

Пенькова Инесса Вячеславовна
д.э.н., профессор
Дзень Дмитрий Александрович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА БАЗЫ ДАННЫХ «1С: ПРЕДПРИЯТИЯ»

1-с предприятие является самым распространенным продуктом на территории стран СНГ. Девять из десяти организаций используют продукты 1С для управления предприятием и ведения учета. Однако безопасность данного продукта находится на очень низком уровне. До версии 7.7 внимание безопасности не уделялось. С выходом версии платформы 8.2 отношение разработчиков к защите информации улучшилось, однако незначительно отразилось на самом продукте.

Существует два основных вида работы программы: файловый вариант и клиент-серверный.

При использовании 1С в файловом формате возникают риски кражи и утечки коммерческой и персональной информации. Связано это с особенностями архитектуры такого типа баз, т.е. с полным доступом ко всем файлам конфигурации и самим файлам для всех пользователей операционной системы. В результате, любой пользователь, имеющий право работать в файловой базе 1С,может скопировать или даже удалить информационную базу 1С двумя кликами мышки.

Сетевая версия является менее уязвимой к физическому воздействию. Также следует выделить общие проблемы безопасности платформы. 1 С:Предприятие поддерживает возможность редактирования, доработки или модернизации программы посредством встроенного языка программирования. Этот язык основан на готовых объектах и классах для работы с протоколами POP3, SMTP, HTTP, FTP, а также с файловой системой, мультимедийными файлами, системными процессами, базами данных, XML, файлами локальной сети и многими другими [1].

Для защиты базы данных 1 С:Предприятия существует несколько методов [2]. Первая заключается в применении отдельных решений для защиты данных, таких как Secret Disk, True Crypt, Aladdin Secret Disk и т.д. Они позволяют ограничить доступ к

конфиденциальной информации при помощи надежного шифрования данных, могут обеспечить соответствия требованиям законодательства, исключают риск несанкционированного копирования базы данных в обход приложения 1С:Предприятие.

Вторым методом защиты является переход с файловых баз 1С на сетевые базы данных. Так как при правильной настройке по надежности, могут сравниться с предыдущей методологией. Для реализации данного метода необходимо привлечение опытных специалистов, которые смогут правильно настроить и зашифровать данные на сервере. Однако стоимость таких работ варьируется от 5 до 10 тысяч долларов.

Таким образом 1 С: Предприятие имеет ряд существенных недостатков в защите данных. Использование базовых версий программы не позволяют обеспечить информационную безопасность. В связи с этим созданы решения, которые позволяют добиться наибольшего уровня безопасности с минимальными затратами.

Список литературы:

1. Гиссин В. И. «1С: Предприятие». / В.И.Гиссин.- Ростов-на-Дону: Изд. Феникс. 2002. - 255с.
2. Информационная безопасность 1С. - [Электронный ресурс]. - Режим доступа: http://efsol.ru/articles/information-security-1c.html //

УДК 004.056.53

Солдатов Максим Александрович
к.ф.- м.н., доцент
Солдатова Светлана Александровна
старший преподаватель
Павлова Владлена Валерьевна
студентка
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

РОЛЬ ИНСТРУМЕНТАРИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Информационно-аналитическая деятельность (ИАД) – это деятельность по аналитико-синтетической обработке и переработке информации различных видов и форм с целью получения качественно нового знания для оперативного обеспечения процесса принятия управленческих решений в различных сферах деятельности.

Предпосылками использования ИАД в Корпоративных Информационных Системах (КИС) является клиент-серверная технология, распределенные базы данных, наличие хранилищ информации, применение современных сетевых технологий и разнообразного инструментария, используемого для сбора, обработки, визуализации и анализа данных. Особенностью систем защиты информации в корпоративных системах является комбинация как минимум трех проблем: защита информации в компьютерных сетях; обеспечение безопасности баз данных; обеспечение безопасной работы систем автоматической обработки информации [1].

Изучив несколько подходов к построению систем защиты информации при помощи ИАД, можно выделить основные инструменты, которые применимы на практике: нейронные сети, деревья решений, методы нечеткой кластеризации, кластерный анализ, ассоциативные правила, алгоритмы ограниченного перебора.

К сегодняшнему дню Российской Академией естественных наук были разработаны совершенно новые эффективные решения в сфере интеллектуальной обработки данных. Создан метаязык “ДИАЛ”, который предназначен для решения проблем безопасного поиска актуальной информации и результативной навигации в Интернет.

Достижения ученых дали возможность повысить качество труда аналитической деятельности и расширить глубину анализа информационного поля, что повлекло за собой значительное усиление прогнозирующей функции работы аналитиков.

Средства защиты информации обязаны обновляться и совершенствоваться. В связи с этим фактом использование ИАД увеличивает эффективность работы системы.

Интеллектуальный анализ данных является дополнительным механизмом в системах информационной безопасности и применяется на начальном этапе.

ИАД – это отличный способ обнаружения неполадок, распознавания атак и прогнозирования изменений в поведении исследуемой модели. Можно заметить, что слаженная работа интеллектуальной составляющей на стратегическом и тактическом уровнях принятия решения о проблеме важнее, чем вычислительная мощность аналитической системы.

Литература:

1. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – Изд-во: ДМК, 2002. – 134 с.

УДК 338.24:334.7

Ячменев Евгений Федорович
к.э.н., доцент
Институт экономики и управления
ФГАОУ ВО "КФУ имени В.И. Вернадского"
Республика Крым, Россия

КОРПОРАТИВНАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА: РЕАЛИИ И ПЕРСПЕКТИВЫ

Актуальность. Начало XXI в. для экономики России характеризовалось чередой процессов, а именно: постсоциалистической трансформацией, глобализацией, когнитивизацией, интеграцией. Каждый из этих процессов внес свой вклад в развитие не только социально-экономический системы страны, но и самого общества. Это общество стали называть информационным, а процессы, ориентированные на упрощение межстрановых перетоков, а точнее, узаконенной утечки людей и институтов, материальных и финансовых ресурсов, которые попадают под усиленное влияние надстрановых управляющих органов, способствуют дестабилизации экономики. «Экономика знаний» стала определяющим фактором страновой конкурентоспособности, движущей силой, основным ресурсом экономического роста и объектом интереса участников глобализации экономики. Интеграцией экономики в целом и отдельных ее систем руководители стран постсоветского пространства увлекались самоотверженно, рапортуя об интеграции в мировую финансовую и банковскую системы, системы учета и отчетности, образования и здравоохранения, позабыв о развитии собственного потенциала. Последствия этих процессов мы сегодня наблюдаем в экономике стран СНГ. При введении санкций именно мировые информационные системы стали предметом шантажа, как государства, так и его граждан (MASTERCARD, VISA). Трансформация привела к деформации или окончательному разрыву устоявшихся связей на разных уровнях, а в клиентеле произошли необратимые процессы. Субъекты рыночной экономики стали уязвимыми для конкурентов, активизировались процессы «рейдерского захвата», информационной опасности, кибератаки. Именно эти негативные последствия вынуждают нас заняться поиском и разработкой информационно-аналитических систем способных решить проблемы не только импортозамещения, информационной безопасности, но и решить проблемы оптимального соотношения между рыночными и административными регуляторами экономики.

Исследованность проблемы. Проблемам разработки, внедрения корпоративных информационно-аналитических систем посвящены работы разных ученых: Г.Б. Клейнер [1] анализирует их весомость в развитии общества, Т.А. Кузовкова, Л.С. Тимошенко [2] задаются вопросом развития информационных коммуникаций, И.А. Лазарев, Г.С. Хижа, К.И. Лазарев [3] определяют связь между информационной экономикой и сетевыми структурами, И. Галахов [4] занимается непосредственно проектированием корпоративных информационно-аналитических систем как инструмента стратегического менеджмента, Е.Ф. Ячменев [5, 6, 7] занимается проектированием информационно-аналитической системы управления как инструмента

оперативного принятия управленческого решения в режиме реального времени в образовательных учреждениях. Вопросы эффективности проектирования информационно-аналитических систем на основе концепции управления корпоративными знаниями изучены не достаточно глубоко.

Целью исследования является анализ существующих подходов к управлению корпоративными знаниями, определение идентичности корпорации, оценить ситуацию на сколько востребованы сегодня корпоративные информационно-аналитические системы управления, их значимость в развитии образовательных учреждений.

Изложение основного материала. Проведя анализ публикаций, которые раскрывают сущность управления знаниями, мы можем выделить три подхода:

1. Технический подход, в котором отдается предпочтение информационным технологиям. В первую очередь – тем, которые предназначены для поиска, хранения, классификации, передачи данных и информации и обеспечивают эффективную работу, обмен знаниями и лучшими практиками. Ключевые акценты – технологии;
2. Организационный подход в основном ориентирован на определение оптимальности структуры организации и существующие в ней бизнес-процессы, чтобы наилучшим образом способствовать эффективному управлению знаниями. Ключевые акценты – структуры и процессы;
3. Человеческий капитал, подход в котором человеческие ресурсы становятся определяющим фактором. Взаимодействия сотрудников, их знания, идентичности, ценности и установки, а также особенности среды и культуры, в которой все они находятся, формируют сложную адаптивную систему интеллектуального капитала. Ключевые акценты – люди и культура.

На практике современное управление знаниями обычно сочетает в себе идеи всех трех подходов, в том или ином соотношении, и чаще всего оказывается направленным на максимально интенсивный обмен знаниями и на создание технических, организационных и интеллектуальных инноваций – а для этого, действительно, важны все ключевые аспекты.

Анализируя более подробно технический подход, оценим значимость информационных технологий. Прежде чем проводить анализ корпоративных информационных систем, необходимо определиться, что же такое корпорация и является ли субъект рыночной экономики, корпоративные информационные системы которого мы анализируем, корпорацией. В классическом понимании корпорация представляет собой совокупность сложных многопрофильных структур и имеет распределенную иерархическую систему управления — корпоративный менеджмент. Структурные подразделения, предприятия, филиалы, дочерние предприятия и административные офисы, входящие в корпорацию, как правило, пространственно удалены друг от друга. Их информационная связь образует коммуникационную структуру компании, основой которой является информационно-аналитическая система.

Является ли университет корпорацией? ФГАОУ ВО "Крымский федеральный университет имени В.И. Вернадского" является сложной многопрофильной структурой и имеет распределенную иерархическую систему управления. Структурные подразделения и филиалы КФУ представлены как образовательными, так и научно-исследовательскими организациями, пространственно они удалены друг от друга. Так, филиалы расположены по всей территории Республики Крым: г. Бахчисарай, Сакский район, с. Прибрежное, пгт. Советский, г. Ялта, г. Армянск, г. Евпатория, г. Севастополь, г. Алушта, г. Керчь, г. Феодосия. Административные офисы и структурные подразделения расположены в разных частях г. Симферополя. Информационная связь между структурными подразделениями и филиалами осуществляется с помощью Интернета и локальных коммуникаций, образуя коммуникационную структуру университета. Все признаки корпорации у образовательного учреждения присутствуют, следовательно, основой его функционирования должна стать корпоративная информационно-аналитическая система.

Информационно-аналитическая система управления — это инфраструктура университета, задействованная в процессе управления всеми информационно-документальными потоками, включающая такие элементы как: информационная модель; регламент ее развития и правила внесения в нее изменений; кадровые ресурсы, обеспечивающие развитие информационной модели; программное обеспечение; аппаратно-техническая база; эксплуатационно-технические кадровые ресурсы; методические рекомендации по использованию программного обеспечения и пользовательские инструкции, регламент обучения и сертификацию пользователей.

Корпоративная информационно-аналитическая система управления (КИАСУ) обеспечивает поддержку принятия управленческих решений на основе автоматизации процессов, процедур и других способов функционирования университета. Кроме того, задачами КИАСУ являются оказание помощи профессорско-преподавательскому составу и ведущим специалистам в анализе текущих проблем, визуальном представлении сложных процессов, прогнозирование потоков и разработке новых образовательных продуктов.

Основным управляющим фактором является процедура принятия решения, на основании результата которой осуществляется воздействие на систему управления (образовательное учреждение, предприятие, корпорацию, компанию, организацию). КИАСУ сама по себе решений не принимает, но, будучи эффективно настроенной, способна поставлять информацию руководителю, лицам, принимающим решения, в том ракурсе, который наиболее подходит для принятия конкретного решения. КИАСУ может взять на себя большинство текущих процедур и процессов в документообороте, движении контингента, учете успеваемости обучающихся и т.д., но далеко не все процессы принятия управленческих решений. В свою очередь, управление без КИАСУ, построенной на современных информационных технологиях, становится все менее эффективным, так как не способно оперативно охватывать весь поток информации для принятия управленческого решения.

Информационная технология, сама по себе, является совокупностью аппаратного и программного обеспечения, технологий хранения информации, сетевых технологий, обеспечивающих коммуникации и связь компонентов системы в единое целое. Все эти ресурсы, используемые в образовательных учреждениях, определяют инфраструктуру информационной технологии, или IT-инфраструктуру, которая является фундаментом для построения КИАСУ.

В составе КИАСУ учитываются средства для документационного обеспечения управления, информационной поддержки предметных областей, коммуникационное программное обеспечение, средства организации коллективной работы сотрудников (создание автоматизированных рабочих мест с соответствующим уровнем доступа) и другие вспомогательные (технологические) продукты (отчеты для разного уровня управления с целью оперативного принятия управленческого решения).

Многопрофильные КИС, к которым в большинстве своем относятся современные КИАСУ, должны в равной, максимально допустимой степени удовлетворять всем структурным подразделениям образовательных учреждений, по возможности обеспечивать сохранность существующих бизнес-процессов, а также методы и структуру управления. Без привлечения автоматизации практически невозможно в режиме реального времени контролировать постоянно меняющиеся баланс финансовых, кадровых, материальных ресурсов, бизнес-процессы, реализуемые проекты (группы проектов, программы) и корпоративные знания, растущие в геометрической прогрессии.

Организационный подход базируется на анализе бизнес-процессов и выборе методов управления знаниями. Методы управления знаниями используют КИАСУ образовательного учреждения как системы небольших коллективов сотрудников, решающих общую задачу, а в роли организующих факторов выступают корпоративные знания и эффективные коммуникации, с общими справочниками и единым хранилищем данных. Главным корпоративным ресурсом управления становится база корпоративных знаний, в которой сотрудники могут оперативно найти информацию для принятия

эффективного управленческого решения и понимания друг друга. Эта база концентрирует в себе коллективный опыт компании и создает основу корпоративных коммуникаций. Основная цель управления — обеспечение координации, коммуникации и быстрого поиска информации для самостоятельного принятия решения. Эта группа методов управления сейчас переживает период бурного развития, и получила общее название «методы управления знаниями».

Что касается интеллектуального капитала, то им в большинстве своем выступают носители знаний. Накопленные знания помогают нам разбираться в различных ситуациях, решать сложные задачи и выполнять трудные задания, учиться на своем опыте и соответственно корректировать свое поведение. Если мы работаем в образовательном учреждении, то наши знания в сочетании со знаниями наших коллег способствуют успешной организации образовательного процесса. Обмен и передача формализованных и неформализованных знаний, лежат в основе образовательного процесса.

Вывод. Таким образом, мы определили, что федеральные образовательные учреждения можно считать корпорациями, а их информационно-аналитические системы – корпоративными.

Установлено, что современное управление знаниями сочетает в себе три подхода (технический, организационный и интеллектуальный), в разных пропорциях. Они обеспечивают максимально интенсивный обмен знаниями и ориентированы на создание технических, организационных и интеллектуальных инноваций.

Список использованных источников:

1. Клейнер, Г.Б. Становление общества знаний в России: социально-экономические аспекты / Г.Б. Клейнер // Общественные науки и современность. – 2005. – №3. – С. 56-69

2. Кузовкова Т.А., Анализ и прогнозирование развития инфокоммуникаций / Т.А. Кузовкова, Л.С. Тимошенко. – М.: Горячая линия – Телеком, 2009. – 224 с.

3. Лазарев И.А. Новая информационная экономика и сетевые механизмы развития / И.А. Лазарев, Г.С. Хижа, К.И. Лазарев. – М.: Издательско-торговая корпорация "Дашков и Ко", 2006. – 240 с.

4. Галахов И. Проектирование корпоративной информационно-аналитической системы / И. Галахов // Журнал "Открытые системы". — Режим доступа: http://www.osp.ru/os/2003/04/182903/ (27.01.2016).

5. Ячменьов Є.Ф. Зовнішні чинники формування вимог щодо розробки інформаційно-аналітичної системи управління вищим навчальним закладом / Є.Ф. Ячменьов // Экономика Крыма. – 2012. – № 3 (40). – С. 75–78.

6. Ячменьов Є.Ф. Реінжиніринг системи управління вищого навчального закладу / Є.Ф. Ячменьов // Культура народов Причерноморья. – 2013. – № 263, Т. 2. – С. 139–143.

7. Ячменьов Є.Ф. Функціональна модель вищого навчального закладу в IDEF0 / Є.Ф. Ячменьов // Бізнес Інформ. – 2014. – № 4. – С. 91–99.

УДК 004.057.2

Бойченко Олег Валерьевич
д.т.н., профессор
Дячук В. С.
студентка 2 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ВНЕДРЕНИЯ СТАНДАРТА МЭК 81650 НА ОБЪЕКТАХ ЭЛЕКТРОЭНЕРГЕТИКИ

На сегодняшний день вопрос состояния защиты данных на объектах электроэнергии в Российской Федерации связан с интеграцией в ЕЭС энергообъектов Республики Крым, как следствие – нарушение единой унифицированной системы стандартизации протоколов передачи данных. Однако, сейчас процесс внедрения современных стандартов защиты информации проходит в условиях реформирования энергосистемы региона.

Протоколы Международной электротехнической комиссии предусматривают возможность гибкой организации передачи данных между устройствами подстанций и системами сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления (АСТУЭ, АСДУЭ, СОТИ АССО, АИИС КУЭ, КСУЭР и др.), а также между самими устройствами.

Область применения стандарта МЭК 61850 — сети связи и системы автоматизации энергосистем общего пользования – подстанций. Данный стандарт содержит руководящие указания для обмена информацией от модели базы данных CDC с использованием IEC 60870-5-101 или IEC 60870-5-104.

Комплекс IEC 61850 содержит:

- стандарт по одноранговой связи и связи клиент-сервер;
- стандарт по структуре и конфигурации подстанции;
- стандарт по методике испытаний;
- стандарт экологических требований;
- стандарт проекта [1].

Стандарт МЭК 61850 применяется в системах автоматизации подстанции. Основное отличие этого стандарта от предшествующих стандартов МЭК заключается в том, что в данном случае речь не идет о простом внедрении нового протокола передачи данных. Основным направлением стандарта является систематизация информационной модели подстанции.

Сегодня при внедрении данного стандарта в ЕЭС России возникает ряд проблем и особенностей. В первую очередь, следует отметить тот факт, что за десять лет существования IEC 81650 было разработано немало научно-технических проектов относительно внедрения данного стандарта на энергообъектах, как коммерческого характера, так и сугубо научного. Результаты таких проектов послужили рабочим материалом для разработки единой системы внедрения стандарта на объектах электроэнергетики с учетом специфики каждого из них [2].

Среди отечественных производителей есть те, кто покупает готовые и более-менее проверенные решения, но в большинстве своем они имеют собственный стенд для испытаний оборудования. Вследствие этого, не всегда реализация, сделанная даже на базе готового стенда, может быть корректно воспринята другими устройствами.

Следующим фактором современного процесса внедрения стандарта являются трудности перевода. Ошибки, возникающие в реализации стандарта, приводят к проблемам при наладке на объекте. Если оборудование ранее не было проверено, проблема ложится на плечи наладчиков (например, устройство релейной защиты не считывается простым опросом). Следовательно, решение — при возникновении сложностей обратиться к первоисточнику. Однако для этого необходимо знать

английский язык и владеть им на высоком техническом уровне, на русский язык стандарт до сих пор не переведен. Безусловно, его надо перевести, но важно сделать это максимально правильно, т.к. у МЭК 81650 есть и первая, и вторая редакции.

Третьим немаловажным параметром при внедрении стандарта является проверка на соответствие и совместимость. Здесь важно отметить, что для успешной совместимости стандарта и системы необходимо в первую очередь корректно реализовать стандарт на каждом устройстве отдельно. Соответствие стандарту подразумевает, что каждое устройство тестируется один раз, выявляются все ошибки, проверяются все функции и сервисы. При проверке совместимости необходимо проверять каждую комбинацию устройств. При такой проверке могут не выявляться ошибки, которые совпадают в обоих устройствах, что, кстати, бывает довольно часто. К тому же проверить можно только те сервисы, которые поддерживают оба устройства.

При проведении испытаний на соответствие можно тестировать устройство не только в штатном режиме, но и с подачей некорректных запросов, при проверке на совместимость подобные возможности очень ограничены.

По результатам проверки на соответствие компания получает сертификат — серьезный документ, который подтверждает все характеристики устройства. И ведущие производители, к примеру, Сименс, Альстом, имеют такие сертификаты [3]. Во втором случае выдается просто отчет о совместимости, который говорит только о том, что два данных устройства могут работать вместе.

Проблема проверки соответствия оборудования стандарту МЭК 61850 встает все острее и острее по мере проектирования инновационных цифровых подстанций, особенно относительно отечественного оборудования. С целью минимизации влияния и дальнейшей ликвидации описанных выше проблем мы предлагаем следующее.

Во-первых, ошибки в реализации стандартов должны выявляться не на этапе наладки и эксплуатации. Они должны быть обнаружены еще на этапе приемки и аттестации оборудования.

Во-вторых, МЭК 61850 — открытый стандарт и это значит то, что его с одной стороны может реализовать любой производитель, а с другой — что любой клиент может проверить, насколько правильно этот стандарт у себя реализовал конкретный производитель. И выгода от использования МЭК 61850 заключается именно в возможности проверки реализации его требований.

Таким образом, методики для испытаний на соответствие стандарта МЭК 81650 должны быть публично утверждены и коррелировать с международными документами. У всех производителей должны быть равные условия, а процессы сертификации и аттестации в свою очередь должны быть возможностью для российских производителей создавать оборудование более высокого уровня.

Список литературы:

1. Alexander Golovin Структура стандарта МЭК 61850 / Alexander Golovin, Alexey Anoshin // [Электронный ресурс]. – Режим доступа: http://digitalsubstation.ru/blog/2012/10/18/struktura-standarta-me-k-61850/

2. Иванов Ю.В. Практический опыт применения и реализации стандарта МЭК 61850 в устройствах противоаварийной автоматики производства ООО «Прософт-Системы». Современное состояние и перспективы. / Ю. В. Иванов, О. С. Бородин, А. Е. Леснов, К.И. Апросин // ООО «Прософт-Системы». – г. Екатеринбург, 2015. – С.34-37.

3. Информационный портал «Dallas Lock – сертифицированная система защиты информации от несанкционированного доступа». Режим доступа: http://www.dallaslock.ru/sub-sert/42-uncategorised/147-sertifikaty-sootvetstviya.html

УДК 004.056.57

Бойченко Олег Валерьевич
д.т.н., профессор
Трофимов Артём Сергеевич
студент 1 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СПОСОБЫ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ

В общем случае, проблемы безопасности операционных систем могут быть представлены целью атаки (по данным Akamai Technologies, за большую часть DDoS-атак несут ответственность представители всего нескольких государств, среди которых на первом месте – США (Рис. 1)); воздействием на операционную систему (пользование легальным получением информации, скрытыми материалами и создание новых каналов получения информации); использованием защищённости (неправильная политика безопасности, ошибки программного обеспечения и предварительно установленная закладка), а также активным и пассивным воздействием на операционную систему. Кроме того проблемы безопасности операционных систем можно классифицировать по источнику возникновения (воровство информации, подбор пароля, превышение полномочий, сбор мусора (уничтоженная информация копируется и просматривается пользователем), а также программные закладки).

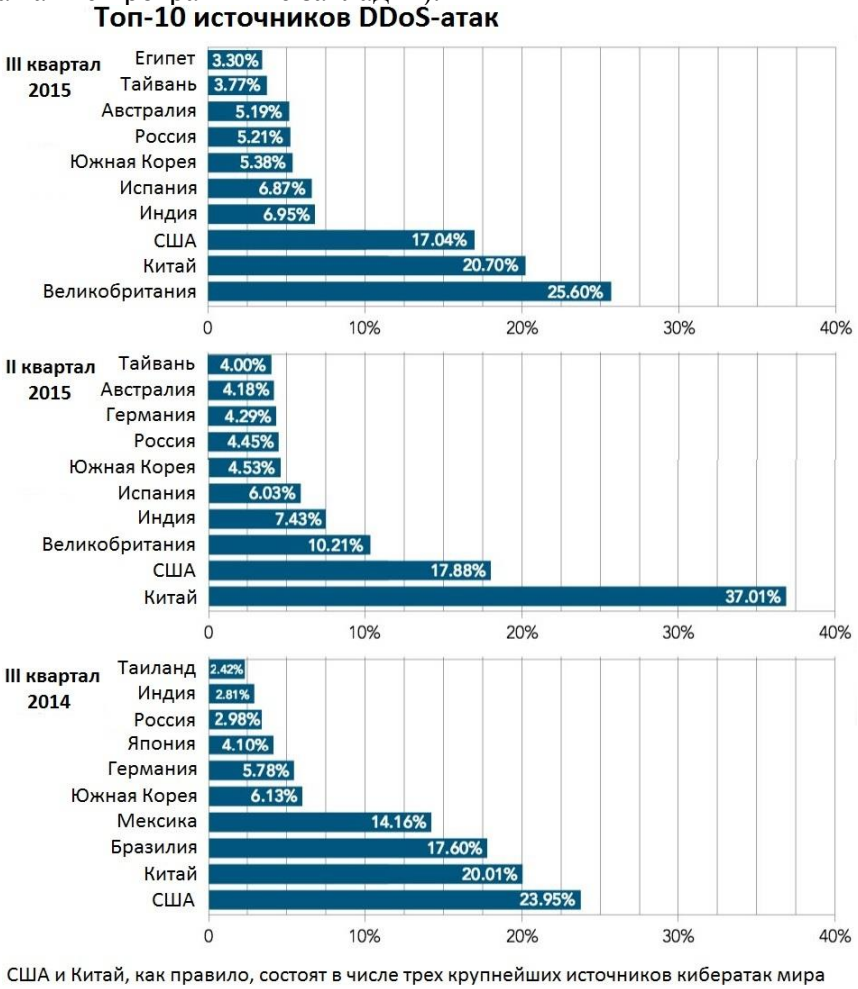


Рис. 1. Топ-10 DDoS-атак в 2014-2015 гг.

Среди эффективных способов защиты операционной системы следует прежде всего выделить такие как:

- контроль функционирования операционной системы;

- организация политики безопасности;
- создание и обновление копий;
- постоянный контроль изменения данных.

Для поддержания политики безопасности операционных систем необходим анализ угроз, а также соответственно сформулированные требования к политике безопасности и ее корректировке.

Кроме того, довольно эффективными способами защиты операционных систем являются:

- идентификация пользователя при входе в систему;
- ограниченные права доступа;
- регистрация событий.

В заключении отметим, что статистика методов, лежащих в основе атак на операционные системы, позволяет выделить некоторые группы, отличающиеся следующими признаками:

- группы, которые позволяют запустить исполняемый код;
- группы, которые запрещают операции чтения или записи файлов или ограничивают права доступа;
- группы, которые приводят к отказу в обслуживании;
- троянские программы.

Таким образом, можно сделать вывод о том, что современные угрозы операционным системам напрямую используют их недостатки, а потому администраторам информационных систем и пользователям систем необходимо усиливать встроенные механизмы защиты.

УДК 004: 658.5

Герасимова Светлана Васильевна
д.э.н., профессор
Аметова Эльвида Наримановна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПОСТРОЕНИЕ ИТ-СТРАТЕГИИ СОВРЕМЕННОГО ПРЕДПРИЯТИЯ

Технологические тенденции и потребности современного бизнеса делают необходимым разработку стратегии предприятия для его успешного функционирования. Современные информационные технологии (ИТ) позволяют снизить затраты предприятия, автоматизируя бизнес-процессы, обеспечивают информационную безопасность, поэтому для поддержания конкурентоспособности у современного предприятия возникает необходимость построения ИТ-стратегии, как оптимального плана достижения бизнес-целей.

Существуют различные походы к построению ИТ-стратегии предприятия. Так, например, согласно одному из таких подходов, в первую очередь, необходимо проанализировать текущее ИТ-состояние, выяснить, в каком из бизнес-процессов, методологии, технологиях деятельности или оборудовании есть так называемые слабые места. Далее предприятию необходимо определить направление, в котором будут развиваться ИТ. Так, например, можно выработать так называемую концепцию развития ИТ, согласно которой увеличение эффективности ИТ-службы, уже существующей на предприятии, является одной из целей ИТ-стратегии. К таким целям можно также отнести автоматизацию бизнес-процессов, реорганизацию существующей ИТ-инфраструктуры и т.д. Немаловажно понимать актуальность долгосрочных целей на этом этапе. Именно они направлены на увеличение конкурентоспособности предприятия в долгосрочной перспективе. Также следует уделить внимание как способам управления

ИТ, их финансированию, так и политике информационной безопасности. На основе анализа текущего состояния ИТ-инфраструктуры и постановки целей развития информационных систем и технологий предприятия необходимо переходить к самому плану достижения целей. На этом этапе возможно создание новых ИТ-подразделений, реструктуризация имеющихся, внедрение различных систем автоматизации (CPM/ERP/MES/PLM) и т.д.

Однако существует принципиально другой подход к построению ИТ-стратегии. Если в первом подходе важным этапом является выделение приоритетных бизнес-процессов, подлежащих автоматизации или реструктуризации, то при втором подходе изучаются тенденции развития ИТ для конкретного бизнеса. Именно учет влияния ИТ на развитие того или иного вида деятельности предприятия является тем ключевым фактором, который позволит увеличить стратегические преимущества.

Такой подход соответствует концепции ITIL. ITIL (Information Technology Infrastructure Library) — библиотека передового опыта в области управления ИТ, изложенная в концепции Управления ИТ-службами — ITSM (IT Service Management), которая предлагает новый взгляд на организацию функционирования ИТ-подразделений, порядок управления этими подразделениями, пути повышения эффективности использования ресурсов [1].

При следующем подходе ключевым фактором при разработке ИТ-стратегии является архитектура предприятия. Понятие архитектура предприятия впервые встречается в статье журнала "IBM Systems Journal" (1987 год). Автор статьи «Структура архитектуры информационных систем» Дж. А. Захман писал, что для снижения затрат и обеспечения успеха бизнеса, все больше зависящего от информационных систем, необходим строгий подход к управлению такими системами. Разработка архитектуры по Захману представляет собой совокупность процедур, состоящих из ответов на вопрос: что (какие данные), как (используемые функции), где (создание и развитие внутренний сети), кто (персоналии), когда и зачем происходит построение ИТ-стратегии. При этом изначально модель предполагалась для информационных систем, однако в дальнейшем Захман назвал её структурой архитектуры предприятия [2].

Рис. 1. Составляющие ИТ-стратегии современного предприятия

При архитектурном подходе построения ИТ-стратегии в основе лежит стратегическая пирамида, где каждому уровню соответствует ИТ-система. Управление эффективностью бизнеса является тем уровнем, на котором системы позволяют контролировать ключевые показатели эффективности, образуя вершину пирамиды. Следующие уровни позволяют оптимизировать ресурсы, управлять ими согласно стратегии, управлять основными, производственными фондами, а также и производством. Базис пирамиды составляют системы управления технологическими процессами. Используя источник [3, с. 74], представим указанную стратегическую пирамиду так, как это показано на рисунке 1.

Таким образом, ИТ-стратегия представляет подробный план достижения целей и задач с помощью портфеля ИТ-решений для повышения управляемости компанией, увеличения эффективности и надежности бизнес-процессов, а также для оптимизации затрат на сопровождение и эксплуатацию ИТ. Выбор подхода к построению ИТ-стратегии и ее корректная реализация - одни из ключевых факторов достижения успеха современного предприятия в 21 веке.

Литература:

1. Карышев М.Ю. Система учетно-аналитических стандартов управления экономическими и производственными процессами в сфере информационно-коммуникационных технологий // Вектор науки ТГУ. – 2011. - № 2 (16). – С.165-168.
2. Захман Дж.А. Структура архитектуры информационных систем // IBM Systems Journal. – 1987. – том 26, № 3. – С. 276-292.
3. Переведенцев Д. А., Матвеева И. В., Романов К. А., Переведенцев К. А. Развитие ИТ-инфраструктуры как фактор повышения эффективности российского предпринимательства // Вестник ИжГТУ. - 2014. - № 1(61) – С.73-74.

УДК

Иванов Сергей Викторович
к.ф.-м.н., доцент
Тупота Елена Сергеевна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МЕТОДЫ ЗАЩИТЫ ОТ DDOS АТАК

Современный веб-ресурс может поддаваться DDoS атакам, обычно такая атака начинается мгновенно и не прекращается – система не отвечает, канал заблокирован, маршрутизаторы перегружены. Эффективно и быстро справится с данной проблемой затруднительно, так как зависит от третьих лиц.

DDoS-атака – вид распределенной атаки направленная на вычислительную систему с целью дальнейшего ее отказа. Данный вид атаки может быть промежуточным шагом для дальнейшего овладения системой.

«Лаборатория Касперского» - компания, специализирующаяся на системах защиты от киберугроз. Были опубликованы исследования по DDoS атакам за 4 квартал 2015 года. Российская Федерация находится на 4 месте в этом рейтинге. По сравнению с показателями третьего квартала отчетного года уменьшилось количество атак на 3,3 %.

Законодательство Российской Федерации крайне слабо по привлечению к ответственности за распределенные атаки.

К DDoS атаке необходимо готовится заранее. К сожалению, на данный момент не существует конкретного метода защиты, необходимо использовать комплексный подход в решении данной проблемы. Для осуществления DDoS атаки используют большое количество «зараженных» компьютеров. Данные компьютеры объединяют в импровизированную сеть «зомби-машин», которые непосредственно и осуществляют данную атаку.

Рассмотрим некоторые примеры защиты сайтов от DDoS атак:

1) В случае, когда на конкретный ресурс идет атака и видно, что большое количество идет на главную страницу. Тогда «компьютеры-зомби, можно обмануть используя javascript-редирект (в случае сайтов, написанных с использованием стандартной структуры web-приложения, написанного на PHP).
   <script type="text/javascript">
   window.location = "http://randomwebsite.ru/index.php"
   </script>
   Результатом таких действий является уменьшение размера файла, с которым соприкасается бот. Обычные пользователи, которые не отключают javascript в браузере, просто перенаправляются на index.php. Еще раз заметим, что это решение временное и применяется непосредственно при атаке.
2) В случае использования, например, Apache HTTP-сервера – кроссплатформенного программного обеспечения в виде свободного веб-сервера. Эта система является общедоступной, надежной и гибкой. Тогда нужно воспользоваться настройками, с помощью которых можно защититься от DDoS атак. Среди них:
   a. TimeOut директива – определяет количество времени, которое Apache будет ожидать: общее количество времени, которое набежит за запрос, количество времени между получением TCP пакетов на POST или PUT запросе, количество времени между ACK на передачах TCP пакетов в ответах. Очевидно, что в случае частых атак это значение параметра надо указывать как можно меньше.
   b. KeepAliveTimeout директива – заданное число времени, которое Apache будет ждать следующий запрос перед закрытием соединения. Так же стоит уменьшить это значение на минимум либо же полностью отключить данную директиву. Все директивы типа TimeOut необходимо проверить и снизить значения в случаи необходимости.
   c. Весьма полезной директивой является – MaxClient. С ее помощью можно указать максимальную пропускную способность клиентов, которые могут одновременно находится на сервере.
3) Сервисы, позволяющие хранить зеркало своих сайтов с помощью их ресурсов. Ярким примером такого сервиса – Akamai (www.akamai.com).
4) Защиту так же можно осуществлять с помощью дополнительного программного обеспечения. Например, DDoS Deflate, DDoS Prevention.

DDoS атаки – очень популярный вид атаки на веб-ресурс. Подготовка к возможным атакам может помочь уменьшить урон от атаки. На практике необходимоь использовать комплексный подход к обеспечению безопасности ресурсов от DDoS атак.

Список использованной литературы:

1. Методы защиты от DDOS нападений [Электронный ресурс]. – Режим доступа: www.securitylab.ru/analytics/216251.php.
2. Касперский К. Техника сетевых атак. Приемы противодействия. Т. 1. – М.: «Слон», 2001.
3. KasperskyLab. «Лаборатория Касперского» отразила одну из мощнейших в истории Рунета DDoS-атак. [Электронный ресурс]. Режим доступа: http://www.kaspersky.ru/news?id=207733980

УДК 003.26

Бойченко Олег Валерьевич
д.т.н., профессор
Карпова Анастасия Александровна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Термин «криптография» (переводится с древнегреческого как «тайнопись», «скрытое письмо») далеко отошёл от своего первоначального значения и в данный момент объединяет методы защиты информационных взаимодействий совершенно различного характера, опирающиеся на преобразование данных по секретным алгоритмам, включая алгоритмы, использующие секретные параметры. На данном этапе невозможно обеспечить полную информационную безопасность, особенно в сети «Интернет», поэтому криптография будет активно развиваться и в будущем.

Целью исследования является проведение анализа существующих проблем в развитии криптографических систем, а также ближайших перспектив их решения.

Наибольшими проблемами являются распределение ключей, шифрование больших объемов данных в реальном времени. Последние инновации в этой сфере – биометрический метод формирования ключей, потоковое шифрование данных, комбинирования алгоритмов шифрования и сжатия информации.

Ещё относительно недавно компьютерное шифрование ориентировалось лишь на текстовые и символьные сообщения, появление мультимедии радикально изменило понятие об объеме шифровальных данных. Для некоторых интерактивных систем, таких как, телеконференция, видео- и аудиосвязь, такое шифрование должно учитывать не только большой объем информации, но и необходимость её передачи в режиме реального времени.

Решение этой проблемы было найдено с помощью технологии потокового шифрования данных. Его отличие от более старых криптосистем в том, что этот метод не ждёт конечного сообщения, а сразу же осуществляет шифрование и передачу файлов. Наиболее очевидным является побитовое сложение входящей последовательности с бесконечным или периодическим ключом, получаемым от какого-то генератора. Примером такого стандарта является RC4, разработанный Ривестом.

Другим, иногда более эффективным методом потокового шифрования является шифрование блоками, то есть накапливается фиксированный объем информации - блок, после чего преобразованный некоторым криптографическим методом передается в канал связи.

В крупных информационных системах наиболее острой является проблема распределения ключей. Существующая технология шифрования с открытыми ключами решает эту проблему, но является трудоемкой, а для шифрования мультимедийных данных совсем не пригодна. Решение этой проблемы предусматривается в ещё разрабатывающейся технологии «блуждающих ключей». Идея метода схожа с принципом работы шифровальных машин военного времени (например, Энигма). После того, как ключ использован в одном сеансе по некоторому правилу, он меняется на другой. Это правило должно быть известно и отправителю, и получателю.

Зная правило, после получения очередного сообщения получатель тоже меняет ключ. Если правило смены ключей аккуратно соблюдается отправителем и получателем, то в каждый момент времени они имеют одинаковый ключ. Постоянная смена ключа затрудняет раскрытие информации злоумышленником.

Сложность реализации этой технологии в выборе эффективного правила смены ключей. Наиболее простой путь - генерация случайного списка ключей. Смена ключей осуществляется в порядке списка. Однако, тогда этот список придется каким-то образом

передавать, что формирует новую проблему. Другой вариант - использование математических алгоритмов, основанных на так называемых перебирающих последовательностях. На множестве ключей путем одной и той же операции над элементом получается другой элемент. Последовательность этих операций позволяет переходить от одного элемента к другому, пока не будет перебрано все множество.

Другой способ решения проблемы распределения ключей усматривается в использовании биометрических данных. Однако и этот способ имеет трудности в реализации: криптография требует точного значение ключа, а биометрические данные всегда имеют погрешность при оцифровке и могут изменяться со временем. Выделяют три системы с такой технологией: с освобождением ключа (Key Release Cryptosystems), со связыванием ключа (Key Binding Cryptosystems) и с генерацией ключа (Key Generation Cryptosystems). В первом виде биометрические данные нужны лишь для аутентификации личности, после чего открывается доступ к ключу, который никак не связан с этими данными. Вторая система значительно надежнее, в ней ключ и биометрические данные непосредственно связаны.

Одному биометрическому эталону соответствует только один биометрический ключ. Системы с генерацией ключа подразумевает, что ключ извлекается непосредственно из биометрических данных пользователя, а не хранится в базе данных. Возможность не хранить ключ, а получать его из биометрических данных пользователя является неоспоримым преимуществом по сравнению с другими существующими методами.

Шифрование, кодирование и сжатие информации используются в различных целях, но отчасти дополняют друг друга и их комплексное использование помогает эффективно использовать каналы связи для надежной защиты предаваемой информации.

Таким образом, ближайшей перспективой решения проблем криптографической защиты данных информационных систем управления, является использование возможности комбинирования алгоритмов шифрования и сжатия информации.

При этом, главным достоинством алгоритмов сжатия, с точки зрения криптографии, является то, что они изменяют статистику входного текста в сторону ее выравнивания. Так, в обычном тексте, сжатом с помощью эффективного алгоритма все символы имеют одинаковые частотные характеристики и даже использование простых системы шифрования сделают текст недоступным для криптоанализа.

УДК 681.5.033.2

Бойченко Олег Валерьевич
д.т.н., профессор
Логвиненко Дмитрий Александрович
студент 1 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МОДЕЛИ ОЦЕНКИ КАЧЕСТВА ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Задачей исследования является анализ математических моделей оптимизации функционирования информационных систем принятия управленческих решений для обеспечения планово-производственной деятельности предприятий и организаций.

Как известно, показателями качества функционирования современных информационных систем принятия управленческих решений является довольно большой перечень факторов, важнейшими из которых являются [1]:

- вероятность предоставления необходимой информации в определенные сроки;
- вероятность отсутствия случайных ошибок в полученной по запросу пользователя информации;

- вероятность сохранения актуальности информации в момент ее использования;
- вероятность предотвращения несанкционированного доступа;
- вероятность сохранения конфиденциальности информации.

Анализ практики использования информационно-поисковых систем специального назначения, которые часто функционируют в условиях неопределенности, наличия довольно существенного влияния внешних факторов (объективной или субъективной природы), а также быстрой смены обстановки и сокращения временных интервалов для принятия управленческого решения, указывает на необходимость разработки мероприятий, направленных на повышение оптимальности функционирования автоматизированных компьютерных систем [2].

В таком случае, одним из направлений усовершенствования действующих автоматизированных систем обработки и предоставления информации является применение математических моделей, основным условием корректности которых является существование и независимость функций распределения, которые описывают характеристики функционирования информационной системы [3,4].

В частности, моделирование процессов представления информации в условиях ненадежности программно-технических средств может быть предоставлена следующим алгоритмом в составе трех этапов:

- моделирование наиболее возможных вариантов допусков, которые сформированы на основе анализа практики применения информационно-телекоммуникационных систем специального назначения (определение перебора известных состояний функционирования информационной системы в реальном времени);
- прогнозирование наиболее возможных вариантов функционирования информационной системы по предоставлению информации (надежное предоставление информации и (или) непредставление информации);
- определение вероятности надежного предоставления информации при выполнении функционального задания следующим порядком

$$P_{над} = \frac{n^2(n^{-1} + w^{-1})}{(\nu + n)},$$

где n^{-1} — среднее время наработки программно-технических средств на отказ; w^{-1} — среднее время возобновления программно-технических средств; ν^{-1} — среднее время выполнения соответствующего функционального задания.

Таким образом, проведен анализ математических моделей оценки надежности и функционирования информационных систем в реальном времени с учетом влияния наиболее вероятных внутренних и внешних факторов, которые снижают эффективность использования автоматизированных систем управления в целом. Предложено использование трехуровневого алгоритма описания модели предоставления информации в условиях ненадежности программно-технических средств.

Список литературы:

1. Євтушок В.П. Організація інформаційного забезпечення збору, аналізу та оцінки оперативних відомостей / В.П. Євтушок // Шляхи вдосконалення ОРД правоохоронних органів. – Додаток №1 до вісника ЛІВС, 2003. - №3. – С. 17-29.
2. Бойченко О.В. Організаційно-правові та програмно-технічні проблеми захисту інформації в автоматизованих системах ОВС України / О.В. Бойченко, К.С. Герасименко // Збірник наукових праць «Проблеми правознавства та правоохоронної діяльності». – Донецьк: Донецький юридичний інститут Луганського державного університету внутрішніх справ ім. Є.О. Дідоренка, 2010. – №2. – С. 68-73.
3. Кормен Т. Алгоритмы: построение и анализ: монография / Т. Кормен, Ч. Лейзерсон, Р. Ривест // М.: МЦНТО, 1999 – 206 с.
4. Портнягин Л.С. Математическая теория оптимальных процессов: монография / Л.С. Портнягин, В.Г. Болтянский, В.Г. Гамкелидзе, Е.Ф. Мищенко. - М.: Физмаггиз, 1961. – 238 с.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Белозуб Владимир Антонович
магистрант
Таврическая академия, факультет математики и информатики
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Необходимым условием построения надежной информационной системы, обеспечивающей одновременную обработки информации разной степени секретности группой пользователей без нарушения прав доступа, является составление набора законов и правил, регламентирующих процессы обработки, защиты и распространения информации в информационной системе. Назовем его политика безопасности. Политика безопасности выступает активным компонентом защиты, включающим в себя анализ возможных угроз и выбор мер противодействия.

Основными элементами формируемой политики безопасности должны стать:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом гарантирует ограничение доступа к объектам, основанные на учете личности субъекта или группы, в которую входит субъект. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т. п.), для дисковых блоков и магнитных носителей в целом.

Метки безопасности. Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, а метка объекта степень закрытости содержащейся в нем информации. Метки безопасности состоят из двух уровней: уровня секретности и списка категорий.

Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если его уровень секретности не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта.

Наряду с *произвольным* и *принудительным* доступом могут использоваться такие механизмы безопасности, как *шифрование (криптозащита), электронная подпись, механизмы контроля целостности данных, механизмы аутентификации.*

В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Умеров Мансур Эскендерович
магистрант
Таврическая академия, факультет математики и информатики
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАЗРАБОТКА ПРОГРАММ И МЕТОДОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Конфиденциальность информации является важным компонентом конкурентоспособности любой организации. Чтобы увеличить уровень надёжности внутренних бизнес-процессов, нужно обеспечить защиту информации от уничтожения (как умышленного, так и случайного), кражи и внесения в неё ненужных изменений. Фальсификация товаров, документов и продукции в последнее время приобрела массовый характер. Чтобы увеличить уровень надёжности, нужно обеспечить защиту информации от уничтожения (как умышленного, так и случайного), кражи и внесения в неё ненужных изменений. Исходя из этого, считаем разработку методов и программ для защиты информации важной и перспективной темой.

Наша цель рассмотреть общие подходы к построению различных методов и подходов для защиты информации, создать программную реализацию по данному типу шифрования, предложить модификацию метода шифрования на основе существующих методов, путем доработки.

Распространенный алгоритм DES предполагает разбивание всего объема данных на блоки длиной 64 бита с последующим шифрованием этих блоков. DES является симметричным алгоритмом: для шифрования и дешифрирования используются одинаковые алгоритм и ключ (за исключением небольших различий в порядке использования ключа). Длина ключа равна 56 битам. (Ключ обычно представляется 64-битовым числом, но каждый восьмой бит используется для проверки чётности и игнорируется). Безопасность полностью определяется ключом, а стойкость шифра – надежностью алгоритма.

На простейшем уровне алгоритм не представляет ничего большего, чем комбинация двух основных методов шифрования: смещения и диффузии. Фундаментальным блоком DES является применение к тексту единичной комбинации этих методов (подстановка, а за ней - перестановка), зависящей от ключа. Такой блок называется этапом. DES состоит из 16 этапов, одинаковая комбинация методов применяется к открытому тексту 16 раз.

Алгоритм был подобран таким образом, чтобы эффективно выполняться на технике 70-х годов прошлого века. В настоящее время ключ в 56 бит не может считаться достаточно устойчивым. Поэтому в программной реализации предполагается использовать ключ длиной 120 бит. Используя его, предполагается выполнение операции XOR частью ключа в 64 бита над всем 64-битный блоком перед выполнением алгоритма DES с 56-битной частью ключа. Отсюда и длина ключа: 64+56 = 120 бит.

Благодаря симметричности операции XOR, модифицированный алгоритм кодирования данных позволит проводить шифрование и дешифрование одним и тем же алгоритмом, что удобно для унификации и минимизации программной реализации.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

Гусельников А. С.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МЕТОДЫ УПРАВЛЕНИЯ ДОСТУПА К РЕСУРСАМ

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [1, 2, 3]. Информационная безопасность включает в себя следующие понятия:

- *Защита* информации – это совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также доступности информации для пользователей.
- *Конфиденциальность* – сохранение в секрете критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций).
- *Целостность* – свойство, при наличии которого информация сохраняет заранее определенные вид и качество.
- *Доступность* – такое состояние информации, когда она находится в том виде, месте и времени, которые необходимы пользователю, и в то время, когда она ему необходима.

Ключевым механизмом защиты информации является контроль доступа к ресурсам, основанный на задании и реализации правил разграничения доступа к ресурсам для пользователей. Задаваемые правила доступа всегда могут быть представлены соответствующей моделью (или матрицей доступа – рис 1.).

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 \ldots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ & \cdots\cdots & & \\ & \cdots\cdots & & \\ 0 & 0 & Зп/Чт & 0 \\ 0 & 0 & 0 & Зп/Чт \end{bmatrix} \end{array}$$

Рис.1 - матрица доступа к ресурсам.

Задача защиты информации не сводится только к контролю доступа; в этой сфере можно выделить так же такие задачи как защита от нарушения ее конфиденциальности, обеспечение ее доступности и целостности. Особое внимание следует обратить на противодействие возможному ее «заражению» макровирусами, что является уже задачей противодействия внешним IT-угрозам.

Для создания системы защиты информации необходимо:

- определить границы управления информационной безопасностью объекта;
- провести анализ уязвимости;
- выбрать контрмеры, обеспечивающие информационную безопасность;
- определить политику информационной безопасности;
- проверить систему защиты;
- составить план защиты;
- реализовать план защиты (управление системой защиты).

Каждое частное решение которое планируется имплементировать, должно прежде всего ориентироваться на специфику системы в которой будет рализовываться мероприятие по защите информации. В тоже время, реализация такого частного решения не должна снижать результирующей эффективности , так как указанная реализация зачастую может приводить к снижению результативности противодействя угрозам в других частях системы.

Список литературы:

1. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.
2. Корольов О.Л., Круліковський А.П. Інтелектуальні методи моделювання процесів управляння проектами / Корольов О.Л., Круліковський А.П. // Ученые записки Крымского федерального университета имени В.И. Вернадского. - Экономика и управление. - 2013. - Т. 1. № 26 (65). - С. 73-86.
3. Модели и информационные системы современной экономики / Апатова Н.В., Бойченко О.В., Герасимова С.В., Пенькова И.В., Сигал А.В., Дюличева Ю.Ю., Иванов С.В., Королев О.Л., Круликовский А.П., Попов В.Б., Рыбников М.С., Солдатов М.А., Акинина Л.Н., Бакуменко М.А. // Под редакцией Н.В. Апатовой. - Симферополь, 2015. - 520 с.

УДК 004.056

Иванов Сергей Викторович
к.ф.-м.н., доцент
Макеев Иван Николаевич
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСНОВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ

Для защиты любой компьютерной системы от несанкционированного доступа к информации и неправомерного вмешательства в процессы их функционирования используются следующие основные методы зашиты [1, с.124]:

- идентификация;
- аутентификация пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация пользователя.

В целях обеспечения возможности разграничения доступа к ресурсам автоматизированной системы компьютерного тестирования (АСКТ) и регистрации событий такого доступа каждый субъект и объект защищаемой автоматизированной системы должен быть однозначно идентифицируем. Для этого в системе должны храниться специальные признаки каждого субъекта и объекта, по которым их можно было бы однозначно опознать [2, с.183].

С одной стороны, идентификация представляет собой присвоение индивидуальных имен, номеров или специальных устройств субъектам и объектам системы, а с другой стороны - это распознавание их по присвоенным им уникальным идентификаторам. Наличие идентификатора позволяет упростить процедуру выделения конкретного субъекта из множества однотипных субъектов [2, с.197].

В свою очередь, аутентификация является проверкой подлинности идентификации субъекта системы. Задача аутентификации заключается в том, чтобы убедится что субъект является именно тем, кем представился. Аутентификация пользователей АСКТ осуществляется путем проверки знания пароля [3, с.241].

Разграничение доступа к ресурсам АСКТ представляет собой порядок использования ресурсов автоматизированной системы, при котором определенные группы пользователей получают доступ к определенным тестам системы в строгом соответствии с установленными правилами [4, с.103].

Можно выделить следующие группы пользователей АСКТ:

- эксперты, создающие тесты по своим направлениям, проводят подготовку тестируемых и анализируют полученные результаты;
- тестируемые – пользователи, проходящие тестирование в разные промежутки времени;
- системный администратор – человек, который занимается программированием данной системы и устраняет возможные ошибки.

Каждый эксперт, который составляет тесты, выполняет однотипные задания, поэтому их можно объединить в группу Экспертов. Не зависимо от количества пользователей, проходящих тест, все они заинтересованы в том, чтобы его пройти и их деятельность складывается в ответах на вопросы теста, следовательно, всех их можно объединить в группу Тестируемые.

Таким образом, описанные механизмы защиты могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты. Успех применения систем защиты информации зависит от наличия в них развитых средств управления режимами работы защитными механизмами, и реализации функций, позволяющих существенно упрощать процессы установки, настройки и эксплуатации средств защиты.

Список используемых источников:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах: уч. пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2007. – 488 с.
2. Халяпин Д.Б. Защита информации. – Баярд М, 2004.- 431 с.
3. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты.? М.: Книжный мир, 2009. - 352 с.
4. Захарова, И.Р. Информационные технологии в образовании: учебное пособие/ И.Р. Захарова. - М.: Издательский центр «Академия», 2008. - 192 с.

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Губарева Дарья Александровна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ЗАЩИТА ПРОФИЛЕЙ ПОЛЬЗОВАТЕЛЕЙ В РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Переход всех бизнес-процессов в сеть Интернет день ото дня набирает все большие обороты. Эта тенденция приводит к тому, что уровень конкуренции среди предприятий возрастает с каждым днем и, тем самым, держит их в «постоянном напряжении». Рекомендации – функция среды электронной коммерции, без которой сегодня невозможно эффективно развивать бизнес в Интернет. Предприятия, в страхе потерять своих клиентов, всеми силами усовершенствуют алгоритмы прогнозирования интересов покупателей.

Рекомендательная система (РС) – это программа, которая способна предугадать будущий выбор пользователя на основе его предыдущих решений. РС позволяет не только улучшить продажи предприятию, но и сильно сэкономить время и силы клиента, поэтому полезна для обеих сторон.

Из-за многокомпонентности понятия «электронная коммерция» (оно включает в себя все финансовые и торговые транзакции, осуществляемые при помощи компьютерных сетей) сложно определить какие именно данные необходимы для построения прогнозов. В зависимости от нужд интернет-предприятия можно выбрать несколько источников информации для предоставления рекомендаций (ими могут быть

как внутренние ресурсы сайта предприятия, так и внешние). К внутренним относятся данные о просмотрах, ответы на вопросы, регистрация с заполнением необходимых полей и создание личного кабинета непосредственно на сайте фирмы. К внешним можно отнести данные поисковых систем и информацию из профилей в социальных сетях. Если в первом случае, система получает данные непосредственно от пользователя, то для обработки внешних данных, ресурс должен «спросить» разрешение. Сначала необходимо ввести личный пароль и логин, выбранной для регистрации, социальной сети, а затем поставить галочку напротив поля «Разрешить», тем самым давая согласие не только на доступ, но и на обработку личных данных.

Сталкиваясь с необходимостью ввода пароля на сайте, не имеющего прямого отношения к конкретной социальной сети, пользователь легко может стать объектом фишинга. Эта схема Интернет-мошенничества основывается на спам-рассылке информации, содержащей прямую ссылку на сайт, который создан по подобию какого-либо известного бренда. Введя данные в эту систему, пользователь может потерять доступ к странице и своей конфиденциальной информации, а мошенники используют её в своих целях. Из-за страха перед такой опасностью, клиент отказывает в доступе к личной информации, а РС сталкивается с проблемой «холодного старта».

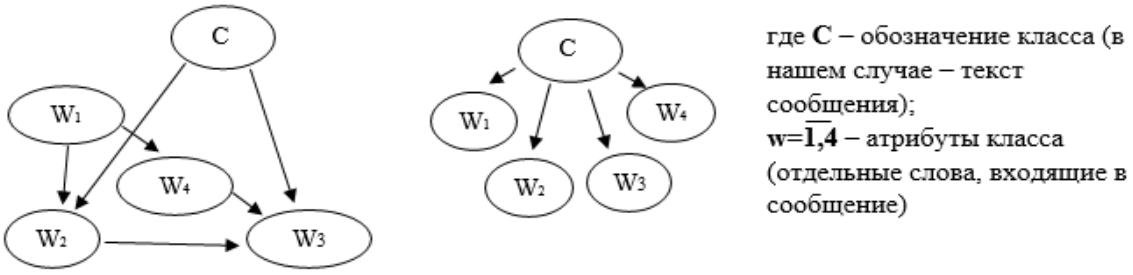
Во избежание потери данных и для обеспечения информационной безопасности, существует ряд методов защиты от фишинга и спам-рассылки. Они берут начало из теории вероятности и ее основных принципов. На практике применяются такие методы, как фильтрация Байеса, контент-фильтры DNSBL, SURBL, SPF, RDNS, Серый список и т.д.[1, с. 12]. Размер словаря фильтров около 50000 слов. Они анализируют состав сообщений и характеристики вложенных в них сайтов по определенным, выведенным ранее параметрам. Основное внимание направлено на выявление вирусов, червей и троянских программ, а спам рассматривается как форма их передачи. Эти методы состоят из фильтров источников, контент-фильтров, анализаторов политики пользователя, программ обучения пользователей, мониторинга систем, а так же методов поиска быстрых решений для систем, подвергающихся атаке, в режиме реального времени.

В контексте фильтрации данных, наиболее широко применяются байесовские сети. Алгоритмы, построенные на их основе не нуждаются в большом количестве данных и могут быть использованы для анализа сообщений и комментариев любой программы, в том числе социальной сети или веб-сайта предприятия электронной коммерции.

Основная задача, решаемая байесовскими сетями – это задача диагностики: наблюдая ряд симптомов и зная их вероятностные зависимости, необходимо найти их наиболее вероятную причину. Идея классификатора состоит в том, чтобы сгруппировать признаки по классам, присвоив им веса. Определив значимость каждого признака, на основе имеющихся входных данных, алгоритм выстраивает правила для новых данных, ранее неизвестных системе. Анализируя взаимосвязанные значения, байесовская сеть и алгоритмы, построенные на ее основе, определяют спам-сообщения и поддельные веб-приложения. На **Рис. 1** мы можем увидеть граф байесовской сети и производного от него наивного байесовского классификатора для определения спама.

Каждый узел графа представляет случайную переменную, а дуги – прямые зависимости между ними. Элементы графа имеют условную зависимость от значения переменных-родителей.

Исследования показали, что спаммеры придерживаются одних и тех же правил изо дня в день до тех пор, пока система защиты не обнаружит взаимосвязь и не предпримет меры защиты. В среднем, поиск таких закономерностей занимает от 8 месяцев до одного года [2, с.831]. На протяжении этого времени пользователь не может быть в безопасности. Для того, чтобы не приходилось с нуля создавать систему и выявлять критерии спам-сообщения или фишинг-сайта, можно использовать уже имеющуюся информацию, определенную ранее.



а) б)

Рис. 1. а) Байесовская сеть и б) Наивный классификатор Байеса

Источник: получено автором по результатам работы [3].

Наличие многолетнего международного опыта позволяет не выводить самостоятельно параметры проверки для создаваемого анализатора. В пример можно привести проект OWASP (Open Web Application Security Project) – это сообщество, которое объединяет инициативных людей со всего мира с целью исследования вопроса безопасности веб-среды. На официальном сайте проекта опубликован Top 10 свойств, которые характеризуют веб-приложение и подлежат контролю другими системами. OWASP рассматривает такие характеристики, как посещаемость ресурса, наличие информации о смене IP-адреса, наличие SSL/TLS-сертификата, доверие к нему и т.д. Эти данные помогают сделать более качественную сеть и позволяют сэкономить время на ее разработку.

Не смотря на все преимущества сетевого бизнеса, его работа усложняется тем, что личного контакта с покупателем Интернет-магазин не имеет. В таких условиях, можно обратиться за советом только к PC, поэтому уровень продаж магазина напрямую зависит от качества предоставляемых рекомендаций. Большое количество веб-приложений (Lamoda, AliExpress, Oriflame, Rozetka и т.д.) даже не требуют регистрации на собственном ресурсе, предоставляя выбор – войти через страницу в какой-либо социальной сети или заново вводить информацию о себе, подтверждая ее телефонным номером или email(ом). Важно, чтобы целью каждого предприятия электронного бизнеса было совершенствование своих алгоритмов защиты клиентов, гарантируя информационную безопасность каждому зарегистрированному пользователю. Это повысит доверие и благоприятно скажется на скорости и качестве взаимодействия обеих сторон - пользователя и компании"

Список использованных источников:

1. Ramachandran A. Understanding the network level behaviour of spammers / Anirudh Ramachandran, Nick Feamster // Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications. — NY : ACM, 2004. — p. 291-302.

2. Jung J. An empirical study of spam traffic and the use of DNS Black lists / Jae Yeon Jung, Emil Sit // Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement. — NY : ACM, 2004. — p. 370-375.

3. Гончаров М. Модифицированный древовидный алгоритм Байеса для решения задач классификации / М. Гончаров [Электронный ресурс]. — Режим доступа: http://www.businessdataanalytics.ru/AugmentedNaiveBayes.htm

УДК 331.08

Пенькова Инесса Вячеславовна
д.э.н., профессор
Аджиев Мидат Османович
магистр
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Технологическая революция, информатизация производственно-хозяйственных процессов вызвали существенное изменение роли человеческого фактора в качестве источника повышения прибыльности предприятия. В научной литературе дается определение оценки трудовой деятельности персонала, как целенаправленному процессу

установления соответствия результатов деятельности личности требованиям исполняемой организационной роли [1, с.27]. Такая оценка целесообразна для: определения профессионализма работника; выработки рекомендаций относительно развития деловых и личностных качеств сотрудников; определения соответствия оплаты труда затрачиваемым работником усилий, его производительности; выявления основных направлений развития персонала; формирования эффективного механизма мотивации труда, в том числе, и на основе защиты интересов сотрудников и обеспечения конфиденциальности его персональных данных.

Анализ эффективности деятельности подразделений управленческого аппарата направлен на соотнесение результатов и затрат, связанных с их функционированием, а также на соизмерение результатов труда с итогами деятельности оцениваемой организации в прошлом и иных организаций с учетом коммерческой тайны. В области подготовки и развития персонала система информационной защиты процесса управления человеческим капиталом призвана выполнять такие функции:

1) перераспределение информации с целью управления развитием навыков и карьерой с помощью найма и дальнейшего постоянного обучения, бесконфликтной командной работой и созданием благоприятных условий карьерного роста, обеспеченного уверенностью в защите личных интересов сотрудника, что имеет информационную природу;

2) сбор и классификация информации относительно своевременного выявления потребности в компетентном персонале и в подготовке или в повышении квалификации персонала;

3) обеспечение подготовки персонала в соответствии с определенными потребностями и информационная защита методов и средств соответствующей подготовки для обеспечения дальнейшей конкурентоспособности фирмы за счет инновационных и/или уникальных методов обучения сотрудников;

4) организация и предоставления всем работникам обучения, сориентированного на достижение целей в рамках общих стратегий организации, в том числе и сфере коммерческой тайны и защиты прав интеллектуальной собственности;

5) перманентность обучения всех категорий персонала изменяющимся особенностям профессиональной деятельности;

6) проведение периодической оценки эффективности подготовки кадров;

7) ведение соответствующих отчетов относительно обучения персонала, его подготовки, опыта и уровня мастерства.

Содержание деятельности структурных единиц управления предприятием, отдельных руководителей или управленцев высшего звена определяется совокупностью или составом основных функций, которые на них возложены организацией.

Таким образом, успешное функционирование системы управления персоналом в организации требует соответствующего информационного обеспечения, способствующего быстрому и защищенному документообороту как внутри организации, так и с внешней средой, а также исполнения возложенных обязательств в необходимый период времени.

Список литературы

1. Морозов М.А. Информационные технологии в социально-культурном сервисе и туризме. / М.А. Морозов– М., 2000.: Оргтехника – 240 с.

УДК 004.58

Пенькова Инесса Вячеславовна
д.э.н., профессор
Шиканова Юлия Александровна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ПРОГРАММНЫЙ АППАРАТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Информационная безопасность (ИБ) предприятия представляет собой комплекс мер для защиты информационных ресурсов от несанкционированного доступа, а также обеспечение их доступности, целостности, конфиденциальности и аутентичности.

Для обеспечения ИБ применяются программно-технические средства защиты информации (СЗИ).

Основные угрозы ИБ связаны с кражей данных, использованием непроверенного ПО, хакерскими атаками, заражением вирусами (например, через электронную почту) и недобросовестностью сотрудников.

К основному ПО защиты информации относятся: программы идентификации и аутентификации пользователей; программы разграничения доступа пользователей к информационным ресурсам; программы шифрования информации; программы защиты информационных ресурсов от несанкционированного доступа.

Для защиты информационных ресурсов обычно используют шифрование и электронную подпись, для поддержания конфиденциальности и целостности информации. При этом шифрование позволяет защитить информацию от несанкционированного доступа даже в случае кражи её носителя. Для сохранения данных при внештатных ситуациях и предотвращения их потери применяются средства резервного копирования для дальнейшего восстановления нормальной работы системы. Наиболее сложной задачей является предотвращение от несанкционированного доступа в системе управления. Она подразделяется на обеспечение защиты ПК, серверов и сетевых соединений.

Под защитой ПК подразумевается предотвращение доступа к информационным ресурсам пользователей, не имеющим соответствующих полномочий. К механизмам защиты ПК относится идентификация пользователей и разграничение их прав (с помощью пароля, биометрических технологий, электронных ключей, смарт-карт).

Защита серверов тоже осуществляется с помощью идентификации. Также фиксируются все действия пользователя, связанные с обращением к серверу для предотвращения и своевременного обнаружения возможных нарушений.

Сетевые соединения защищаются посредством аутентификации ПК и серверов, основанной на применении цифровой подписи и шифрования. Для контроля над информационными потоками между ИС предприятия и внешней средой (например, сети Интернет) может использоваться технология межсетевого экранирования, которая позволяет отслеживать данные из внешней среды и проверять их на наличие угроз.

Подводя итог, отметим, при организации защиты информации необходимо непрерывно совершенствовать СЗИ, т. е. постоянно контролировать функционирование системы, выявлять слабые стороны и возможные каналы утечки информации, обновлять механизмы защиты в зависимости от изменения характера угроз. Это означает, что поддержание ИБ не может быть разовым мероприятием и требует постоянного контроля и усовершенствования.

УДК 651 : 330

Попов В. Б.
к.ф.-м.н., доцент
Медведев Д. С.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

КОМБИНАТОРНЫЕ АЛГОРИТМЫ И МЕТАЭВРИСТИКИ В АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ IT-КОМПАНИИ

Цель работы. Данная статья касается вопросов автоматизации бизнес-процессов компании по регенерации картриджей.

Для достижения поставленной цели нужно было выполнить ряд задач. Необходимо было проанализировать и охарактеризовать объект и задачу автоматизации технологического процесса выбранного IT-предприятия. Далее требовалось сформулировать и решить задачу оптимизации, для чего необходимо было исследовать предметную область (технологические процессы) и описать состояние ее автоматизации, сформулировать требования к системе, смоделировать прецеденты и разработать техническое задание к системе. Следующей задачей являлась разработка проекта автоматизированной системы, который включает в себя разработку архитектуры и обоснование технологий автоматизированной системы, моделирование данных, разработку алгоритмов, моделирование состояния и поведения, а также проектирование структуры классов и компонентов системы. Был разработан прототип автоматизированной системы. Разработка прототипа предусматривает разработку интерфейса, реализацию программного кода и качества, создание документации по проекту и оценку количественных характеристик проекта и ожидаемых эффектов от его применения.

В ходе выполнения задания был разработан сайт для автоматизации процесса по регенерации картриджей. Сайт позволяет клиентам делать заказы через Интернет. Для менеджера фирмы, благодаря веб-сервису «Google Maps», проект позволяет находить маршруты с минимальной длиной к клиентам, вести учет ресурсов. Сайт создан с использованием технологии ASP.NET в Visual Studio Ultimate 2012 при использовании шаблона проектирования MVC4 Internet Application. Также была разработана BPMN-диаграмма и блок-схема процесса работы сервиса по регенерации картриджей. Созданы UML-диаграммы: прецедентов, конечных автоматов, последовательности, классов, объектов и компонентов. В результате была получена модель данных.

Математическая модель в проекте должна определять кратчайший маршрут от офиса компании к клиентам, то есть решать задачу коммивояжера. Задача коммивояжера заключается в нахождении выгодного маршрута, проходящего через указанные города хотя бы по одному разу. В условиях задачи указываются критерий выгодности маршрута (кратчайший, самый дешевый, совокупный критерий и т.д.) и соответствующие матрицы расстояний, стоимости и т. д. Обычно задано, что маршрут должен проходить через каждый город только один раз, в таком случае решение находится среди гамильтоновых циклов. Задача сводится к решению задачи линейного программирования (1):

$$\min(max)\, F = \sum_{j=1}^{n} c_j x_j \qquad (1)$$

где c_j - весовые коэффициенты, x_j - искомые значения, n - количество переменных.

$$\sum_{j=1}^{N} a_{ij} x_j \begin{Bmatrix} \leq \\ = \\ \geq \end{Bmatrix} b_i \ \left(i = \overline{1,m}\right) \qquad (2)$$

$$x_j \geq 0 \ \left(j = \overline{1,n}\right),$$

x_j – целые числа.

где m – количество ограничений, a_{ij} - коэффициенты в ограничениях, b_i – свободные члены.

Алгоритм решения задачи:

- Симплексным методом решают задачу (1) (без требований целочисленности переменных). Если среди элементов условно-оптимального плана нет дробных чисел, то это решение является оптимальным планом задачи целочисленного программирования. Если задача (1) не имеет решения (целевая функция ограничена, или система ограничений несовместима), то задача (1) - (2) также не имеет решения.
- Когда в условно-оптимальном плане дробные значения, то выбирают одну из не целочисленных переменных x_i и определяют ее целую часть $[x_i]$.
- Записывают два ограничения, отсекающие нецелочисленные решения:

$$x_i \leq [x_i]$$

$$x_i \geq [x_i] + 1 .$$

- Каждое из полученных неравенств присоединяют к ограничениям исходной задачи. В результате получают две новые целочисленные задачи линейного программирования.
- В любой последовательности решают обе задачи. В случае, когда получено целочисленное решение хотя бы одной из задач, значение целевой функции этой задачи сопоставляют с начальным значением. Если разница не больше заданного числа ε, то процесс решения может быть закончен. В случае, когда целочисленное решение получено в обеих задачах, то с решением начальной сопоставляется тот, который дает лучшее значение целевой функции. Если же в обоих задачах получено нецелочисленные решения, то для дальнейшего ветвления выбирают ту задачу, для которой получено лучшее значение целевой функции и осуществляют переход к шагу 2.

Для программной реализации задачи коммивояжера был использован сервис Google Maps. Математическая модель рассчитывает общую сумму заказанных услуг, в зависимости от количества выполненной работы и рассчитывает маршрут, с минимальным путем.

Анализ литературы позволяет сделать вывод, что принципиальная трудность задач дискретной оптимизации делает, по-видимому, невозможным построение эффективных точных алгоритмов для большинства классов задач. К тому же задачи дискретной оптимизации, как математические модели практических ситуаций выбора наилучших решений не тождественны ситуации, а являются ее приближенным описанием, поэтому и решать задачи дискретной оптимизации разумно с той же степенью приближения к экстремуму. Метаэвристики являются мощным и чрезвычайно популярным классом оптимизационных методов, позволяющих находить решения для широкого круга задач из различных приложений. Эффективность метаэвристик состоит в их способности решения сложных задач без знания пространства поиска, именно поэтому эти методы дают возможность решать трудноразрешимые задачи оптимизации. Упрощенно можно рассматривать метаэвристики как алгоритмы, реализующие прямой случайный поиск возможных решений задачи, оптимальных или близких к оптимальным, пока не будет выполнено некое условие или достигнуто заданное число итераций. Метаэвристики – это общие эвристики, позволяющие находить близкие к оптимальным решения различных задач оптимизации за приемлемое время. Метаэвристики – это стратегии, которые управляют процессом поиска решения. Цель метаэвристики состоит в эффективном исследовании пространства поиска для нахождения (почти) оптимальных решений. Метаэвристические алгоритмы варьируют от простых процедур локального поиска до сложных процессов обучения. Метаэвристические алгоритмы являются приближенными и, как правило, недетерминированными. Метаэвристические

алгоритмы могут включать механизмы избегания попадания в ловушку в ограниченной области пространства поиска. Метаэвристики могут быть описаны на абстрактном уровне (т.е. они не предназначены для решения конкретных задач). Метаэвристики могут использовать предметно-ориентированных знания в виде эвристик, которые находятся под контролем стратегии верхнего уровня. Современные метаэвристики используют сохраненный в памяти опыт поиска решения для управления поиском.

УДК 004.056.5

Солдатов Максим Александрович
к.ф.-м.н., доцент
Иванова Анна Геннадьевна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время для обеспечения информационной безопасности используют большое количество алгоритмов, важным элементом которых являются случайные числа. Это позволяет снизить риск взлома системы и потери данных.

Генерация псевдослучайных чисел может применяться по следующим направлениям:

Генераторы сессий(PHPSESSID). Для безопасности при создании сессии используется уникальный идентификатор. Обычно он генерируется PHP – сервером, но злоумышленник может украсть его с сервера. Поэтому существуют дополнительные способы генерации и хранения идентификатора, самым распространенным из которых является повторная генерация идентификатора.

Генерация текста для CAPTCHA. Здесь речь идет о генерации специальных изображений против спам-ботов. Алгоритмы для такой генерации могут быть разнообразными, но все базируются на основных принципах и не являются чересчур сложными. Генерировать необходимо шум и текст, которые впоследствии будут искажаться.

Шифрование. Для шифрования и дешифрования используются специальные ключи, которые обеспечивают безопасность шифра от взлома. Для получения таких ключей при шифровании используются методы генерации псевдослучайных чисел.

Генерация соли для криптографии - случайное число соли используется, как правило, для шифрования “в одну сторону”, а также для хэширования паролей. Это случайное значение используется как вектор инициализации в криптографии.

Генератор паролей. Генераторы паролей используются для создания паролей, предлагаемых пользователю, но чаще всего для угадывания уже существующего пароля. Для обеспечения большей безопасности при создании паролей накладывают ограничения на минимальный размер пароля, а также проверку на «сложность» пароля. Многие сложные генераторы имеют дефекты и проблемы с хранением и проверкой подобранных паролей, поэтому проще всего использовать линейный метод перебора паролей.

Таким образом, можно сделать вывод, что генерация псевдослучайных чисел является неотъемлемой частью обеспечения информационной безопасности. Главным недостатком таких чисел является то, что они только имитируют случайные числа, но по факту являются зависимыми от алгоритмов и факторов, выбранными разработчиками. Решением этой проблемы продолжают заниматься многие крупные компании и отдельные ученые. Не смотря на это, псевдослучайные числа значительно повышают уровень безопасности любой информационной системы.

Использованные источники:
1. Пару слов о генерации случайных чисел в PHP [электронный ресурс]- Режим доступа: http://ruseller.com/lessons.php?id=1720&rub=32
2. Подробно о генераторах случайных и псевдослучайных чисел [электронный ресурс].- Режим доступа: http://habrahabr.ru/post/151187/

Таратухина Татьяна Сергеевна
студентка
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Симферополь, Россия

СОВРЕМЕННЫЕ ПОДХОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ КОММЕРЦИИ

На сегодняшний день безопасность является ключевым вопросом при внедрении и использовании систем электронной коммерции (ЭК) [3, 4]. Психологический фактор, связанный с осознанием угрозы потенциального мошенничества, остается основным препятствием для использования Интернета в качестве средства проведения коммерческих операций.

Пользователи и специалисты до сих пор не рассматривают Интернет как безопасную среду. Опросы показывают, что наибольшей потенциальной угрозой является несанкционированное получение персональных данных при использовании открытых каналов связи Интернет. По данным разработчиков платежной системы VISA около 23% транзакций ЭК так и не производится из-за боязни клиента ввести собственную персональную информацию при работе, например, с электронным магазином персональную информацию о клиенте[1]. Анализ литературных источников показывает, что для обеспечения необходимо выполнить следующие три условия:

- исключить возможность перехвата персональной или банковской информации во время транзакции;
- исключить возможность извлечения этой информации из баз данных;
- исключить возможность использовать "украденную" информацию в собственных целях.

Для защиты от перехвата, для защиты информации во время транзакции используют как симметричные, так и асимметричные криптоалгоритмы. Вместе с тем используются дополнительные каналы связи отличные от Интернет - каналов: факс, телефон, обычная почта и т.д.

Учитывая, что зарубежное и Российское законодательство приравнивает цифровую подпись к рукописной, широкое распространение получило аутентификация транзакций на основе концепции цифровой подписи. Преимущество электронной цифровой подписи в том, что она позволяет однозначно идентифицировать пользователя. Недостаток же заключается в том, что электронная цифровая подпись также может быть уязвима для мошенников. Злоумышленники могут добраться до ключа от цифровой подписи, заразив компьютер вредоносным программным обеспечением.

При рассмотрении возможности перехвата интересующей информации, нельзя не исключить "человеческий фактор", поэтому одновременно с программно-аппаратными средствами необходимо использовать и организационные, обеспечивающие охрану информационных ресурсов, исключение шантажа, контроль за паролями и т.д.

Для защиты информации от перехвата используются протокол шифрования SSL (Secure Sockets Layer) и SET (Secure Electronic Transaction). SSL применяется для шифрование данных, передаваемых от компьютера пользователя в систему банка и обратно. Широко используемый и ставший практически обязательным в интернет-торговле протокол SSL позволяет всем участникам торговли спокойно передавать самую разную информацию. При попытке перехвата данных они будут закрыты шифром, взломать который за сколько-нибудь адекватный промежуток времени невозможно.

Протокол SSL надежно защищает информацию, передаваемую через Интернет, но все же он не может уберечь частную информацию, хранимую на сервере продавца, — например, номера кредитных карт. И если сервер не защищен и данные не зашифрованы, то возможен несанкционированный доступ к частной информации и дальнейшее использование ее в мошеннических целях.
В дополнение к использованию протокола шифрования передаваемых данных участники интернет-коммерции используют такие способы идентификации держателя карты, как проверка CVV2/CVK2-кодов (CVV2-код для карт платежной системы Visa и CVK2 — для MasterCard).

Однако протокол SSL ввиду технических особенностей считается менее надежным. SET более защищенный протокол, но технологически сложный и дорогой. Поэтому его повсеместное внедрение не осуществляется и вопрос безопасности остается открытым.

Ещё одним методом защиты интернет-банкинга являются одноразовые пароли, получаемые в банкомате. При такой системе защиты, кроме обычного логина и пароля, для входа в систему и подтверждения операций пользователь должен ввести одноразовый пароль, список которых он может получить в банкомате своего банка.

С точки зрения безопасности такая система имеет преимущество — чтобы совершать операции по карточному счету через интернет-банкинг, лицо должно как минимум иметь в наличии непосредственно саму карту, а также знать PIN-код, чтобы получить список паролей в банкомате.

Вместе с тем нельзя не учесть ряд недостатков такой системы защиты. Одним из них является то, что список паролей, распечатанный в виде чека из банкомата, необходимо хранить для подтверждения будущих операций. А это значит, что при его потере необходимо приобрести новый.

Также существуют одноразовые SMS-пароли — это система, при которой каждая операция, осуществляемая посредством он-лайн — банкинга, должна быть подтверждена одноразовым паролем, который пользователь получает в SMS-сообщении на мобильный телефон. При этом мобильный номер должен быть «привязан» к номеру счета.

Эта система имеет несколько преимуществ. Во-первых, она достаточно проста в использовании — нет необходимости в специальном оборудовании, а процедура подтверждения операции занимает всего несколько минут. Во-вторых, она позволяет обезопасить учетную запись от использования злоумышленниками — даже если мошенникам станет известен логин и пароль для входа в систему, они не смогут получить доступ к деньгам, а пользователь узнает о попытке провести несанкционированную операцию из SMS-сообщения [2].

Существует еще множество других средств защиты электронной коммерции, однако на данный момент невозможно достичь полной безопасности данных систем. Но тем не менее, использование существующих систем защиты обеспечивает создание относительно безопасной среды для проведения различных операций в сфере ЭК.

Список литературы:

1. Голдовский И. Безопасность платежей в Интернете - СПб: Питер, 2010. - 240 с.
2. Резниченко Е., Безопасность Интернет-банкинга: практические аспекты [Электронный ресурс]. - Режим доступа: http://www.prostobank.ua/internet_banking/stati
3. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.
4. Корольов О.Л., Круліковський А.П. Інтелектуальні методи моделювання процесів управляння проектами / Корольов О.Л., Круліковський А.П. // Ученые записки Крымского федерального университета имени В.И. Вернадского. - Экономика и управление. - 2013. - Т. 1. № 26 (65). - С. 73-86.

Антропова Анна Александровна
студентка
Королёв Олег Леонидович
к.э.н., доцент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Симферополь, Россия

ИНТЕРНЕТ-МАРКЕТИНГ И КОНФИДЕНЦИАЛЬНОСТЬ

Интернет-маркетинг недавно появившееся течение маркетинга, образовавшееся в следствие развития информационных технологий и электронной коммерции. Под интернет-маркетингом подразумевают любую деятельность в рамках рынка, направленную на продвижение товаров (работ и услуг) от производителя к потребителю с использование комплекса мер в сети Интернет, т. е. не только баннерную рекламу и public relations, но и методики проведения маркетинговых исследований в Интернете, в том числе изучение спроса и потребительской аудитории, освоение алгоритмов формирования и обеспечения высокой эффективности рекламных кампаний, способов правильного позиционирования торговой марки на рынке[1].

Стремительно увеличивающаяся аудитория сети Интернет в России, состоящая в основном из молодой и достаточно обеспеченной части общества, делает Рунет еще более привлекательным как средство маркетинговых коммуникаций [5].

Однако в значительной мере уменьшает эффективность интернет-маркетинга низкий уровень доверия пользователей. Ключевым моментом определения уровня доверия к компании, которая функционирует в виртуальной среде является защита конфиденциальной информации пользователей сети Интернет.

Таким образом, отсутствие гарантии такой защиты означает, что кто-либо может перехватить передаваемые данные, в том числе и персональные, и попытаться извлечь ценную информацию (к примеру, данные о кредитных картах) [2]. Конфиденциальная информация Пользователей обычно указывается при вводе регистрационных данных и может быть использована для подбора продуктов или услуг согласно потребностям. Информация такого рода не может быть передана каким-либо образом третьим лицам, кроме случаев указанных в «Согласии с рассылкой» или предусмотренных законодательством РФ.

Согласно Статьи 15 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015), обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено[3].

Также предусмотрено создание Реестра нарушителей прав субъектов персональных данных, для отражения сведений об интернет-сайтах, содержащих информацию, обрабатываемую с нарушением законодательства РФ в области персональных данных [4]. Данный проект основывается на постановлении Правительства РФ от 19 августа 2015 г. № 857 "Об автоматизированной информационной системе "Реестр нарушителей прав субъектов персональных данных".

Однако перехват может произойти и в момент передачи информации или после ее совершения. Для предотвращения таких инцидентов используются технологии шифрования данных, а также протокол SSL (Secure Socket Layer) и стандарт SET (Secure Electronic Transactions) [1]. Протокол SSL обеспечивает защиту данных, передаваемых в сетях TCP/IP по протоколам приложений за счет шифрования и аутентификации серверов и клиентов. Стандарт SET обеспечивает надежную защиту номеров кредитных карт и другой конфиденциальной информации, пересылаемой через Интернет, активно

применяется для обеспечения защиты номеров кредитных карт и другой конфиденциальной информации, пересылаемой через Интернет.

Подводя итог, можно отметить, что интернет-маркетинг весьма перспективен в России, так как аудитория пользователей стабильно увеличивается. Компании, не безразличные к своему рейтингу и репутации, проводят постоянный мониторинг развития международных требований для контроля над доверенными данными, полученными в сети Интернет-ресурса, соблюдая все мировые стандарты в обеспечении сохранности информации. Это предполагает не только выполнение всех инструкций, норм и доведения их сведения Уведомления о конфиденциальности, но и повышение квалификации сотрудников. Провалы в выполнении подразумеваемых и декларированных обязательств во взаимоотношениях с клиентами, не только негативно влияют на репутацию, но и влекут за собой юридическую ответственность.

Список использованной литературы:

1. Петрик Е.А. Интернет-маркетинг - М.: Московская финансово-промышленная академия, 2004 – 299 с.
2. И.В. Успенский Интернет-маркетинг Учебник.- СПб.: Изд-во ПГУЭиФ, 2003.
3. Федеральный Закон О Персональных Данных [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/
4. Вступил в силу закон о хранении и обработке персональных данных россиян с использованием серверов, находящихся на территории России [Электронный ресурс]. – Режим доступа: http://www.garant.ru/news/648095/#ixzz3yf2qCDJp
5. Круликовский А.П. Индекс готовности к информационному обществу как базис приоритетного развития крымского региона / Круликовский А.П., Садретдинов О.Р. // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. - 2014. - Т. 4. № 27 (66). - С. 104-109.

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Гусейнова Айтан Ризван кызы
студентка 4 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

По данным на начало 2016 г. число пользователей Интернет в мире насчитывает 3,2 миллиарда человек (всего населения – 7,2 млдр. чел.), в России – это 84 млн. пользователей старше 16 лет. Практически каждый, имеющий доступ к Интернет, также входит в одну из социальных сетей, общаясь через нее со своими знакомыми и приобретая многочисленных виртуальных «друзей», которых никогда не видел, но получая от них разнообразную информацию. По сети быстро распространяется как интересная, полезная, так и вредная, особенно для молодых людей, информация, влияющая на их мировоззрение и общественное поведение. В связи с этим становится актуальным решение двух задач: во-первых, защита личных данных в сети от несанкционированного доступа и распространения и, во-вторых, защита от информационного воздействия, способного нанести вред физическому и психическому здоровью, а также репутации пользователя.

Для информационной защиты россиян разработана Доктрина информационной безопасности Российской Федерации, определяющая интересы своих граждан следующим образом: 1) интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность; 2) интересы общества в информационной сфере заключаются в обеспечении интересов общества в этой сфере, упрочении демократии, создании правового социального государства, достижении и

поддержании общественного согласия, в духовном обновлении России; 3) интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека (гражданина) в области получения информации. Одновременно требуется использование этой сферы только в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, безусловного обеспечения законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества [1, с. 54]. В Концепции информационной безопасности Республики Казахстан говорится, что в социальных сетях часто происходит манипулирование информацией, предвзятое комментирование различных событий, формирование враждебного для личности информационного фона, что создает угрозу национальной безопасности государства.

Социальные сети как новый мировой феномен уже начал внедрять средства собственной защиты, например, Facebook разработал сайт Internet.org. Специалисты сайта решают задачи улучшения доступа к информации, выкладываемой пользователями сети, а также задачи защиты этой информации, в том числе, фотографий и сведений личного характера. Команда специалистов исследует самые разные технологии, в том числе с использованием дальнемагистральных высотных самолётов, спутников и лазеров, разрабатывает новые мобильные приложения.

Проблема информационной защиты в социальных сетях заключается также в невозможности использовать новые протоколы и программы защиты данных при выходе в сеть с устройств устаревших моделей, особенно мобильных телефонов.

Литература

1. Кондратова Е.Г. Социальные сети и корпоративная информационная безопасность // Безопасность информационных технологий. 2013. № 2. С. 54-57.

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Гусейнова Шафига Ризван кызы
студентка 4 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ

В официальной литературе отсутствуют данные по общим объемам виртуального предпринимательства в России и количеству виртуальных предприятий в целом. Это связано с тем. Что нет четкого понимания, что такое «виртуальное предприятие» на государственном уровне, поскольку практически все предприятия, и не только торговые, имеют свои сайты в Интернет и так или иначе занимаются электронным бизнесом. Суммарный оборот интернет-магазинов в России за 2014 год составил 612 млрд рублей. В прошлом году суммарный оборот интернет-магазинов оценивался в 470 млрд рублей. Таким образом рост оборота составил 31%. По данным InSales.ru, в 2014 году в России работало около 43 тысяч розничных интернет-магазинов, в которых совершаются заказы. Рейтинг 100 топ-магазинов, работающих в Интернет, представили 29 октября 2015 компании Data Insight и Ruward [1]. Сто крупнейших интернет-магазинов России – это основа электронной торговли в нашей стране. На них приходится 58% от всех заказов и сопоставимая сумма оборота. Крупнейшие из них имеют десятки тысяч заказов в день, опережая вторую сотню по числу заказов на два порядка. Именно эти сто магазинов фактически определяют сегодня будущее Интернет-торговли, появление новых сервисов, появлений новых условий и принципов работы. По максимальному индексу безопасности, равному 8,75, первыми стали магазины Юлмарт, Lamoda и E96.ru. Индекс безопасности включает четыре тематические группы: «Наличие угроз для

пользователей», «Обеспечение безопасности сайта», «Защита персональных данных», «Репутация надежности сайта». Каждому фактору был присвоен свой вес независимо от других факторов. Индекс безопасности вычислялся как сумма весов всех проверяемых факторов. Проверка сайтов производилась при помощи облачного сканера SiteSecure, а также специально разработанными для исследования программными средствами и, по нескольким факторам, вручную. Облачным сканером SiteSecure сканировались все доступные для индексации страницы сайта. Сканирование проводилось однократно в течение второй половины сентября 2015 года. SiteSecure является технологическим лидером рынка защиты сайтов для малого и среднего бизнеса от финансовых потерь и простоев, вызванных интернет-угрозами. Мы постоянно наблюдаем за безопасностью более 80 000 коммерческих сайтов. На основе накопленной информации эксперты SiteSecure опубликовали исследования безопасности сайтов и состояния безопасности разработки в веб-студиях в 2014 и 2015 годах.

Информационные риски виртуальных предприятий можно условно разделить на три категории: 1) риски, связанные с использованием информационных компьютерных систем на предприятии в различных сферах его деятельности (внутренние - производство, учет, управление); 2) риски, связанные с выходом предприятия в компьютерную сеть Интернет (внешние риски, являющиеся наиболее существенными для виртуальных предприятий); 3) риски, связанные с использованием информационных технологий и большой долей влияния человеческого фактора (маркетинговые риски). Последний вид риска вязан также с ценовой политикой предприятия, поэтому его целесообразно рассмотреть как самостоятельный [2, с. 163].

Литература

1. Рейтинг ТОП-100 Интернет магазинов России 2015. Электронный ресурс. Режим доступа: http://www.ruward.ru/ecommerce-index-2015/
2. Апатова Н. В., Малков С.В. Рискология виртуального предпринимательства: Монография. — Симферополь: - 2013. — 316 с.

УДК 004.056.5

Бойченко Олег Валерьевич
д.т.н., профессор
Броцкая Лолита Олеговна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ФИШИНГ В КОРПОРАТИВНОЙ СРЕДЕ

Хищение личных идентификационных данных представляет повышенный интерес в преступной среде. Это обусловлено достаточно простым доступом к данным за счет использования современных цифровых технологий. Наиболее часто злоумышленники используют специально сформированные сообщения для заманивания своих жертв в ловушки (фишинг), с последующей кражей идентификационных данных пользователей.

Фишинг представляет собой процедуру рассылки электронных сообщений, замаскированных под надёжный источник (официальные сайты банков или социальных сетей), целью которой является создание условий для получения конфиденциальных данных пользователя. Фишинговое письмо обычно содержит ссылку на сайт, которая является точной копией Интернет-банка или другого финансового учреждения. В случае успешной фишинг-рассылки, пользователи вводят запрошенные данные, попадающие в последствие злоумышленнику. Чаще всего целью фишинговых мошенников являются логины, пароли и номера кредитных карт пользователей.

Фишинговые электронные сообщения в корпоративной среде обычно представляют собой таргетированную атаку, хорошо продуманы и реализованы. Таргетированные (целевые) атаки – это атаки, которые направлены в отношении

конкретных коммерческих организаций или государственных ведомств. Данные атаки не носят массовый характер и готовятся длительное время. Преступники изучают информационные системы объекта, а также использующееся в них программное обеспечение.

В настоящее время растёт процентная доля целевых фишинговых атак, которые организованы через рассылку писем по электронной почте, в которых можно выделить конкретную организацию или группу лиц. Целевые пользователи получают хорошо разработанные фишинговые сообщения, которые заставляют человека ввести конфиденциальные сведения типа логина и пароля, предоставляющие доступ к корпоративным сетям или базам данных с важнейшей информацией.

Помимо запрашивания учётных данных, целевые фишинговые письма могут также содержать вредоносное ПО. Например, при нажатии определённой клавиши могут загружаться программы для отслеживания всего того, что жертва будет вводить клавиатурой. Проведение целевых фишинговых атак требует от преступников больше времени, чем в проведении традиционных фишинговых атак. Мошенники должны получить доступ или украсть списки адресов электронной почты для целевой организации, а потом создать правдоподобные письма, привлекающие получателей с целью получения их персональных данных.

Точечный фишинг является самым распространённым типом таргетированной атаки, а потому представляет особую угрозу информационной безопасности корпорации. Характеризуется высоким уровнем создания условий для введения в заблуждение даже тех пользователей, которые очень серьёзно подходят к вопросам безопасности. Кроме того, такой тип фишинговой атаки является базисом для проникновения хакеров в корпоративную сеть.

Следует также отметить, что для разработки фишинговых почтовых сообщений используются методы социальной инженерии, располагая получателя к доверию и достигая основной цели по получению персональных данных пользователя. При этом, для атаки формируется таргетированное письмо, содержащее персонализированную информацию и ссылку на сайт. Для рассылки используется поддельный сайт или поддельный адрес отправителя. Кроме того, мошенники применяют изощренные способы, заставляющие жертву перейти на сайт, где пользователи оставляют нужную информацию или загружают на компьютер вредоносное ПО. Большее количество сообщений содержат URL-адреса, по которым получатель переходит на вредоносные сайты, имеющие такой же вид, как их действующие аналоги. Другим способом фишинговой атаки является применение психологического приема, основанного использовании в сообщении фраз с угрозами каких-либо неприятных последствий в случае не выполнения рекомендаций перехода по ссылке или обещания бонусов от известного сервиса.

Проведенный анализ проблематики противодействия фишингу в корпоративной среде показывает, что основную долю фишинговых сообщений составляют вредоносные файлы, офисные документы, которые содержат макросы с функционалом.

В настоящее время особую опасность приобретает сетевой фишинг, что обусловлено стремительным ростом онлайн сервисов и широкими возможностями мошенников к организации фишинговой атаки даже в условиях абсолютной безопасности сервиса.

Универсального способа, позволяющего обеспечить высокий уровень информационной безопасности и противодействия фишинговым атакам, в настоящее время не существует. В таком случае актуальным является разработка комплекса мер для пользователей, позволяющего создать условия для уменьшения риска кражи персональной информации пользователя.

По мнению авторов, в состав комплекса информационной защиты от фишинга, необходимо включить следующие элементы:

- постоянный визуальный контроль пользователями строки адреса с изображением замка в окне браузера и сертификата безопасности используемого сайта;

- установка контроля за почтовыми вложениями и ссылками, соблюдение мер предосторожности и уведомление о всех подозрительных случаях службы технической поддержки;
- использование для передачи персональной информации шифрованного соединения с адресом, который начинается с "https://", а не с "http://";
- обращаться только к сообщениям, подписанным цифровой сигнатурой.

Таким образом, соблюдение комплекса мер информационной безопасности от фишинга позволит создать условия необходимого уровня защиты персональных данных пользователей в корпоративной среде.

УДК 004.056

Иванов Сергей Викторович
к.ф.-м.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Защита WEB-приложений является одной из самых сложных, важных и постоянно меняющих свой характер задач, стоящих перед разработчиками. При этом, говоря о защите web-приложения, чаще понимают не только защиту от внешних факторов, атак, но и устойчивость работы самого приложения в целом.

Обеспечение безопасной и устойчивой работы приложения закладывается с самого начала разработки. В этом вопросе важно все: и архитектура самого приложения, и архитектура всей системы, и закладываемые принципы коммуникаций, и используемые технологии и многое другое.

Любое web-приложение можно разделить на клиентскую часть и серверную. Методы и подходы защиты клиентской части нельзя рассматривать как надежную и устойчивую защиту в силу одного простого факта: исполняемый код находится на стороне клиента и при желании он может быть изменен так, как это нужно злоумышленнику. Поэтому организацию безопасности на клиентской стороне нужно рассматривать скорее как «первую линию обороны», которая позволяет отсеивать нежелательные обращения к серверной стороне и тем самым снимает с нее часть нагрузки.

К организации безопасной и устойчивой работы приложения на клиентской стороне можно отнести такие моменты, как:

- обеспечение проверки вводимых данных;
- «экранирование» выводимых символов;
- скрытие паролей;
- демонстрация только безопасной информации;
- отсутствие прямых ссылок на ресурсы и т.д.

Обеспечение безопасности на серверной стороне приложения является более сложной и трудоемкой задачей. К основным моментам относятся:

- использование безопасных HTTS/SSL соединений;
- ограничение доступа к базе данных (запрет доступа извне, доступ только для сервера приложения);
- шифрование хранимой в базе данных информации;
- использование безопасных и стабильных версий сервера приложений и постоянный мониторинг обновлений;
- использование только безопасных и рациональных подходов к разработке приложения (избегание SQL-инъекций, небезопасных подключений ресурсов и т.п.);
- обеспечение целостности данных;

- обязательная аутентификация пользователей;
- логирование действий пользователей;
- гарантия отлько авторизованного доступа и т.д.

Одним из важных моментов в безопасности приложения является полноценное и грамотное тестирование. Если безопасность действительно критична, заказчик понимает ее важность и располагает некоторыми финансовыми ресурсами, то использование услуг специализированных профессиональных компаний, которые проводят полномасштабную и всестороннюю проверку безопасности – это наиболее рациональное и правильное решение.

Разработка действительно безопасного приложения является очень трудоемким процессом, требующим ответственного отношения всех участников разработки, постоянного контроля качества и соблюдения протоколов безопасности.

Список использованных источников

1. Иванов С.В., Москалева Ю.П. Разработка бизнес-приложений // Ученые записки ТНУ, Экономика и управление – 2011 – Том 24 (63). №1. — С. 54-59
2. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.
3. Hildenbrand, Tobias and Heinzl, Armin and Geisser, Michael and Klimpke, Lars and Acker, Thomas "A Visual Approach to Traceability and Rationale Management in Distributed Collaborative Software Development" In: Heinzl, Armin and Dadam, Peter and Kirn, Stefan and Lockemann, Peter (eds): Lecture Notes in Informatics, P-151, PRIMIUM - Process Innovation for Enterprise Software, Koellen, Mannheim – 2009 – pp. 161-178.

УДК 004.056

Иванов Сергей Викторович
к.ф.-м.н., доцент
Карпова Анастасия Александровна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ВИРТУАЛИЗАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В наше время информационные технологии становятся всё более важными и незаменимыми. Они упрощают жизнь, помогают экономить и оптимизировать нашу деятельность. Одной из таких технологий является виртуализация. Виртуализация в информационных технологиях – это процесс представления набора вычислительных ресурсов или сущностей, абстрагированный от аппаратной реализации. Виртуализация обеспечивает логическую изоляцию всех процессов, выполняемых на едином физическом ресурсе. В последние несколько лет технологии виртуализации стали очень популярными. В связи с этим возникает вопрос: как влияет эта технология на информационную безопасность? Чтобы дать ответ на этот вопрос, необходимо рассмотреть классификацию виртуализации.

Первым и наиболее распространённым видом является виртуализация компьютера. В данном виде выделяют технологии программной и аппаратной виртуализации. Программная – это вид виртуализации, который полностью основывается на специальных программах, и в свою очередь разделяется на динамическую и паравиртуализационную. Первый подвид основывается на оперативной замене проблемных команд гостевой ОС гипервизором в режиме реального времени. Паравиртуализация считается более эффективной, по сравнению с динамической, и подразумевает предварительную модификацию ядра гостевой ОС. Программная виртуализация является наименее безопасной и имеет особенности, создающие серьезные проблемы ИБ:

- гипервизор и хостовая ОС представляют единую точку отказа;

- программного реализация гипервизора более уязвима к атакам, чем аппаратно-программная реализация;
- такая виртуализация не обеспечена защитой на аппаратном уровне по технологии TPM.

Более современной является технология аппаратной виртуализации. Она решает проблемы возникающие в программном виде. Крупные вендоры разрабатывают свои платформы виртуализации, которые основываются на технологиях аппаратной виртуализации Intel VT (VT-x), AMD-V. Например, компания Intel внедрила в одном из чипсетов технологию безопасности LaGrande/TXT со спецификацией TPM 1.2. Данная технология позволяет контролировать целостность программно-аппаратной среды компьютера. А в технологии AMD-V реализован специальный защищенный режим запуска монитора виртуальных машин.

Второй вид виртуализации – виртуализация сетей, которая представляет собой преобразование сетевых ресурсов типа фрейма, пакета, сессии и управление ими. При этом используются канальный, сетевой, транспортный и сессионный уровни модели OSI. Виртуализация сетей возможна по технологии виртуальной частной сети (внешняя) и по технологии виртуальной локальной вычислительной сети (внутренняя). Внешняя имеет глобальный характер применения, так как работает на сетевом уровне и объединяет множество сетей в одну виртуальную, а внутренняя – работает на локальном уровне. Основными целями виртуализации сетей являются: разделение и управление потоками информации, сетевая изоляция, сегментирование сети, защита информации при ее передаче по сети.

Третий вид – виртуализация приложений. Этот вид основывается на формировании нескольких независимо работающих приложений или их пользовательских представлений. Целями виртуализации приложений являются: отделение приложений от операционной системы, предоставление возможности для выполнения приложений в различных средах. Проще говоря, при такой виртуализации приложение выполняется на удаленном сервере, а его пользовательский интерфейс отображается локально. Данная виртуализация широко используется в современности для управления клиентскими приложениями и защиты конфиденциальных данных.

Несомненно, виртуализация в информационной безопасности играет большую роль, хотя её и нельзя выделить как отдельный механизм. Виртуализацию сетей на базе общепринятых и частных протоколов можно выделить в отдельное направление сетевой безопасности.

Виртуализация представлений служит хорошим методом изоляции пользователя и сервера, что важно при их локализации в двух зонах, противоположных по условиям ИБ. Положительной стороной является то, что между сервером и рабочей станцией нет обмена программным кодом, что исключает риск передачи вредоносных программ. Технология аппаратной виртуализации, использующая модуль TPM и спецификации TCG для реализации доверенной среды, позволяет создавать безопасные разделы с проверкой идентичности и целостности виртуальной машины и всех задействованных в ней программно-аппаратных компонентов.

Одним из главных направлений применения технологии виртуализации в задачах ИБ является обеспечение доступности информации. Данная задача решается посредством виртуализации серверов и систем хранения данных. Виртуализация экономит значительные инвестиции по сравнению с физическим дублированием и резервированием оборудования.

Литература

1. Иванов Д.В. Виртуализация общества.Версия 2.0. [текст]/ Д.В.Иванов – Санкт-Петербург: Петербургское востоковедение, 2002 г. – 224 с.

2. Турулин И.И. Виртуализация (изоляция вычислительных процессов)[текст]: учебное пособие/ И.И. Турулин – Таганрог: ТТИ ЮФУ (бывший ТРТИ, ТРТУ), 2012. – 40 с.

3. Нил Макалистер. Виртуализация серверов[текст]/ Нил Макалистер// «Computerworld Россия» - 2007г. - №9 – с. 19-22

4. М. Тим Джонс. Виртуальный Linux. Обзор методов виртуализации, архитектур и реализаций [текст]/ . М. Тим Джонс //[Электронный ресурс]/ режим доступа: http://www.ibm.com/developerworks/ru/library/l-linuxvirt/index.html

Королёв Олег Леонидович
к.э.н., доцент
Бояджан Сергей Владимирович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

ТЕХНИЧЕСКИЕ СРЕДСТВА БЕЗОПАСНОСТИ ИНТЕРНЕТ-ПРОЕКТОВ

Прежде чем рассматривать технические средства безопасности, необходимо разобраться в том, что такое «Интернет-проект». Интернет-проектами считаются только лишь те проекты, которые созданы в сети Интернет как самостоятельные. Выделяют три главных вида Интернет-проектов: торговые, используемые для продвижения и продажи товаров, контентные, которые предоставляют доступ к информации и новостям, а также интернет-сервисы, которые предоставляют разнообразные услуги. [1.с 82, 3]

Технические средства защиты (ТЗС) разделяются на два больших класса со своими спектрами задач: защита от несанкционированного доступа (НСД) и защита информации от утечки техническими каналами.

Защита от НСД может осуществляться различными способами:
- системы разграничения доступа к информации;
- системы аутоинтефикации и идентификации;
- аппаратные ключи;
- системы сигнализации;
- средства блокировки устройств и интерфейсов ввода-вывода информации.

Защита информации от утечки по техническим каналам может осуществляться следующими средствами:
- установка активных систем зашумления;
- создание контролируемых зон;
- использование экранизированного оборудования;
- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров.

Всегда существует риск проникновения злоумышленников в ваш Интернет-проект различными способами для разнообразных целей, однако использование данных мероприятий позволит значительно снизить этот риск [2].

Список использованной литературы:

1.Тавридович, Станислав Александрович. Оптимизация WEB-сайта интернет-магазина с использованием генетического алгоритма : диссертация ... кандидата экономических наук : 08.00.13 Санкт-Петербург, 2004 159 с. : 61 04-8/4870

2 [Электронный ресурс]. – Режим доступа: dic.academic.ru/dic.nsf/emergency/2939

3. Модели и информационные системы современной экономики. Монография / Апатова Н.В., Бойченко О.В., Герасимова С.В., Пенькова И.В., Сигал А.В., Дюличева Ю.Ю., Иванов С.В., Королев О.Л., Круликовский А.П., Попов В.Б., Рыбников М.С., Солдатов М.А., Акинина Л.Н., Бакуменко М.А. // Под редакцией Н.В. Апатовой. - Симферополь, 2015. – 520 с.

УДК 330

Королев Олег Леонидович
к.э.н., доцент
Лукьянова Мария Альбертовна
студентка
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

В современном мире находятся тысячи угроз и опасностей, которые подстерегают нас на каждом шагу, и Всемирная сеть, которая стала неотъемлемой частью нашей жизни, не является исключением. На данный момент в мире киберпреступность имеет глобальные масштабы и является проблемой каждой страны, потому что практически каждая компания имеет свой сайт в Интернет, а злоумышленник в сети может легко оставаться абсолютно анонимным. Пропорционально росту бизнеса растет и количество угроз. Однако, как показывает многолетняя практика, большинство атак происходят из-за стандартных ошибок валидации или выявления злоумышленниками уязвимости в установленных компонентах программного обеспечения компании, из-за халатности системных администраторов, которые используют пароли и настройки, установленные по умолчанию. [5]

OWASP (Open Web Application Security Project) – это международная некоммерческая организация, которая сосредоточена на анализе и улучшении безопасности программного обеспечения[1]. Этим сообществом был разработан список десяти самых опасных векторов атак на веб-приложения - OWASP TOP-10:

1) Наиопаснейшими векторами атаки являются инъекции (Injections). Недостаточная проверка данных пользователем, дает возможность злоумышленнику внедрить в форму веб-интерфейса приложения специальный код, содержащий кусок SQL-запроса, который дает ему возможность получить доступ к базе данных и читать, изменять, удалять информацию, непредназначенную для него[1].

2) Недочет системы аутентификации и хранения сессий (Broken Authentication and Session Management). Для различия пользователей веб-приложений используются сессионные куки, т.е. после того, как Вы введете логин и пароль, приложение Вас авторизует и в хранилище браузера сохранится специальный идентификатор, который в будущем браузер будет предъявлять серверу при каждом запросе страницы вашего веб-приложения. В случае, если ваш идентификатор попадет в руки злоумышленника, а в системе не были реализованы необходимые проверки, то он может получить доступ в систему с правами вашего аккаунта[1].

3) Межсайтовый скриптинг – XSS (Cross Site Scripting) является одной из ошибок валидации данных пользователя, которая позволяет получить JavaScript код на исполнение в браузер пользователя. Такие атаки часто называют HTML-инъекциями. От SQL-инъекций они отличаются тем, что внедряемый код исполняется в браузере пользователя. В следствии чего, злоумышленник получит возможность украсть вашу сессионную cookie, а также данные, вводимые в формы на зараженной странице. Через JavaScript киберпреступники могут изменять данные, расположенные на атакованной странице[1].

4) Небезопасные прямые ссылки на объекты (Insecure Direct Object References). Суть этой атаки заключается в том, что при выводе конфиденциальных данных для доступа к объекту используется идентификатор, передающийся в открытом виде в адресной строке браузера, а проверка прав доступа к объектам не проводится. Эксплуатация этой уязвимость очень проста, потому что для ее реализации достаточно лишь перебирать число в адресной строке браузера и получать результат[2].

5) Небезопасная конфигурация (Security Misconfiguration). При отсутствии в настройках сервера правильной и включенной опции cookie_httponly или использовании

паролей, установленных по-умолчанию, злоумышленники могут получить доступ к сессионной cookie через JavaScript, что позволит им читать и изменять данные, вводимые пользователем в браузер[2].

6) Незащищенность критичных данных (Sensitive Data Exposure). Данные, которые передаются по протоколу HTTP не шифруются, а, при прохождении данных от пользовательского компьютера до веб-сервера, данные пройдут много разных узлов, на каждом из которых может затаиться сниффер - программа, которая считывает весь трафик и передает злоумышленнику[2].

7) Отсутствие функций контроля доступа (Missing Function Level Access Control). Суть этой атаки состоит в том, что отсутствует проверка на наличие надлежащего доступа к запрашиваемому объекту. Если параметры запроса плохо проверяются, злоумышленники легко могут подделать запрос для доступа к данным без полагающегося разрешения[2].

8) Межсайтовая подделка запроса (Cross-Site Request Forgery, CSRF/XSRF). Вектор атаки CSRF, который иначе называют XSRF, дает возможность злоумышленнику под чужим именем выполнять действия на таком сервере, нак котором не реализованы дополнительные проверки. Например, для перевода средств на другой аккаунт, в некоторых платежых системах есть страница, имеющая такой вид: demobank.com/transfer_money.jsp?transfer_amount=1000&transfer_account=123456789, где transfer_amount – это сумма для перевода, а transfer_account – это номер аккаунта, на который должны быть переведены средства. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на вышеуказанную страницу платежной системы. В результате чего – деньги будут перечислены на счет злоумышленника[3].

9) Использование компонентов с известными уязвимостями (Using Components with Known Vulnerabilities). В основном веб-приложения пишутся с использованием специальных библиотек или «фреймворков», поставляющихся сторонними компаниями. Эти компоненты имеют открытый исходный код, т.е. они есть не только у Вас, но и у миллионов людей по всему миру, которые штудируют исходный код на предмет уязвимостей[3].

10) Непроверенные переадресации и пересылки (Unvalidated Redirects and Forwards). Веб-приложения часто переадресуют пользователя с одной страницы на другую. В процессе должны использоваться проверяемые параметры с указанием страницы конечного назначения переадресации. Но без необходимых соответствующих проверок, злоумышленник может использовать такие страницы для переадресации жертвы на подложный сайт, который, например, может иметь очень похожий интерфейс, но украдет ваши данные кредитной карты или другие конфиденциальные данные[3].

Список использованных источников:

1. Скембрей, Дж., Шема, М. Секреты хакеров. Безопасность Web-приложений - готовые решения/ Скембре, Дж., Шема М – М.: Издательский дом "Вильямс", 2003. — 384 с.

2. Хабрахабр «OWASP TOP-10: практический взгляд на безопасность веб-приложений» [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/company/simplepay/blog/258499/

3. Ховард, М., 19 смертных грехов угрожающих безопасности программ. Как не допустить типичных ошибок/ М. Ховард - ДМК Пресс, 2006. – 216 с.

4. Применение энтропии при моделировании процессов принятия решений в экономике / Королев О.Л., Куссый М.Ю., Сигал А.В. Монография // Под редакцией А.В. Сигала. - Симферополь, 2013. – 168 с.

5. Королев О.Л. МОДЕЛЬ ОЦЕНКИ РИСКА КИБЕРАТАКИ ДЛЯ ВИРТУАЛЬНОГО ПРЕДПРИЯТИЯ / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.

Королев Олег Леонидович
к.э.н., доцент
Феськова Юлия Дмитриевна
студентка
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

СОВРЕМЕННЫЕ ПОДХОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БИЗНЕСА

Одним из видов электронного бизнеса считается электронная коммерция. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка и расчеты) реализовывается с помощью Интернета [1]. Поэтому в такой интерпретации как правило полагают, что покупка относится к электронной коммерции, если, как минимум, маркетинг (организация спроса) и расчеты производятся средствами Интернета. Более узкая трактовка понятия "электронная коммерция" характеризует системы безналичных расчетов на основе пластиковых карт.

Принципиально новый подход к осуществлению электронных платежей сегодня заключается в немедленной авторизации и шифровании финансовой информации в сети Интернет с использованием протоколов SSL (Secure Sockets Layer) и SET (Secure Electronic Transaction).

Протокол SSL предполагает шифрование информации на канальном уровне, а протокол SET, разработанный компаниями VISA, MasterCard и др., - шифрование исключительно финансовой информации. Поскольку сеть Интернет рассчитана на одновременную работу миллионов пользователей, то в коммерческих приложениях "в чистом виде" невозможно использовать ни традиционные системы, основанные исключительно на "закрытых ключах" (DES, ГОСТ 28147-89 и др.), ни методы шифрования только на "открытых ключах", в том числе и российский стандарт электронной подписи.

Применение одних закрытых ключей невозможно в связи с тем, что раскрытие (перехват) даже одного ключа сразу же приведет к "взлому" всей системы защиты. Поэтому при реализации электронной коммерции в Интернет вместе с системами шифрования с помощью закрытых ключей используются системы шифрования с помощью открытых ключей. Это связано с тем, что шифрование только открытыми ключами требует больших затрат вычислительных ресурсов. Поэтому лучше всего шифровать информацию, передаваемую по сетям, с помощью закрытого ключа, который генерируется динамически и передается другому пользователю зашифрованным с помощью открытого ключа.

Для защиты сделок в Интернет в настоящее время организованы специальные центры сертификации. Они следят за тем, чтобы каждый участник электронной коммерции получал уникальный электронный "сертификат", в котором с помощью ключа центра сертификации подписан открытый ключ данного участника коммерческих сделок.

Работа по проведению новых подходов обеспечения безопасности ведется, но сложности еще остаются. Эта деятельность предполагает создание большого числа все более сложных алгоритмов шифрования, специальных программ для перехвата и нейтрализации атак. Специалисты в этой области, как в нашей стране, так и за рубежом много полезного уже осуществили в сфере разработок новых программных средств для «отслеживания» и «улавливания» атак, чего нельзя не заметить. Однако у систем электронной коммерции всё еще остаются много не устраненных уязвимостей. Поэтому их необходимо тщательно изучать и стараться быстрее устранять. От этого зависит как-никак объем продаж, а значит, и доходность данного сектора коммерции.

Список литературы:

1. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.

УДК 330

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Иванова Анна Геннадьевна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ПРЕИМУЩЕСТВА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УЧЕТА ПОСЕТИТЕЛЕЙ НА ПРЕДПРИЯТИИ В СФЕРЕ УСЛУГ

В настоящее время автоматизация деятельности стала для предприятий обычным делом. Но далеко не все используют её в своей работе. Это связано с незнанием всех преимуществ, которые дает автоматизация.

Все больше и больше предприятий в сфере услуг переходят на автоматизированную систему учета посетителей. Раньше такой учет велся вручную и записывался на большом количестве бумаги, использовались папки и картотеки. Для хранения такой документации необходимо много места, что является большой проблемой для небольших предприятий. Введение автоматизированной системы учета решает не только проблему пространства, но и значительно снижает время занесения и обработки информации. Такая система дает возможность накапливать информацию, сортировать её, выводить интересующие данные по запросам и составлять статистические и другие виды отчетов.

Создание автоматизированной системы ведения учета может осуществляться как недорогими, а иногда и бесплатными средствами, так и специализированными системами, включающими целый комплекс оборудования и уникального программного обеспечения.

Автоматизированные системы ведения учета имеют удобный интерфейс, автоматически рассчитывают стоимость услуг для отдельных посетителей, рассчитывают прибыль предприятия, дают возможность регистрации и бронирования мест [1, с.368].

Важным преимуществом систем учета является наличие системы авторизации. Получить доступ к информации может только зарегистрированный пользователь с определенным уровнем доступа. Этот уровень определяется привилегиями, которые назначаются администратором сети в соответствии с корпоративной политикой. Это позволяет обезопасить данные от просмотра посторонними лицами.

Высокий уровень защиты информации имеют онлайн-системы учета, размещенные на удаленных серверах. Примером такой системы является CRM система для автоматизации спортивных, танцевальных и детских развивающих клубов «Отмечалка», представляющая пример SaaS (software as a service — программное обеспечение как услуга) проекта, созданного на базе облачных технологий [2].

Использование системы «Отмечалка» страхует предприятие от потери данных, связанной с неисправностью оборудования, техногенными проблемами, так как все данные хранятся в дата-центрах Германии и Нидерланд. Таким образом, местные службы или конкуренты не смогут получить доступ к конфиденциальные данные предприятия и и личным данным посетителей. Сохранность информации обеспечивается за счет ежедневного резервного копирования информации.

Но не стоит забывать и о том, использование западных платформы для разработки и хостинга приложений приводит к тому, что данные фактически хранятся за пределами России. Такая ситуация увеличивает геополитические риски.

Облачные вычисления позволяют строить информационные системы для учета без несанкционированного использования программного обеспечения, радикально снизить затраты на построение центров хранения обработки данных. Самым большим недостатком Облачных технологий является вопрос обеспечения безопасности хранимых данных клиентов. Для пользователей облачных технологий должен быть интересен стандарт ISO 27002, который можно использовать и при построении облака SaaS, но в любом случае необходима разработка специального стандарта для информационной безопасности облачных вычислений.

Список использованных источников:

1. Модели и информационные системы современной экономики / [Апатова Н. В., Бойченко О. В., Королев О. Л. и др.] ; Под редакцией Н. В. Апатовой. — Симферополь, 2015. — 520 с.
2. Отмечалка – онлайн автоматизация обучающих и спортивных заведений / Сайт CRM системы «Отмечалка» [Электронный ресурс]. — Режим доступа: https://otmechalka.com/, свободный. (Дата обращения: 10.01.2016).

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Павлова Владлена Валерьевна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ОСНОВНЫЕ ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Безопасность - это защита от нанесения ущерба либо меры его уменьшения. Безопасность означает сохранение системой постоянства, неуязвимости и возможности саморазвития.

В электронной коммерции информационная безопасность является одним из важнейших составляющих ведения своего бизнеса. Основным объектом информационной безопасности является коммерческая информация фирмы. Поэтому прежде чем организовывать бизнес-деятельность в сети Интернет надо позаботиться о продуманной системе защиты информации.

Изучив данные об угрозах в сохранении конфиденциальности, выясняется, что посягательство на интересы субъектов может быть и неумышленное, что усложняет выбор компонентов системы защиты от компьютерных преступлений.

Чтобы обеспечить успешную деятельность, требуется правильно сбалансировать три важных составляющих: правовую, организационную и инженерно-техническую безопасности.

Выделять виды угроз в компьютерной сфере в век технологического развития очень сложно. Мошенники каждый день совершенствую свои действия, и придумывают новые методы достижения целей.

Однако, чтобы ориентировать компании в выборе направления схем защиты в электронной коммерции, можно выделить наиболее применяемые и устоявшиеся методы посягательств на информацию:

1. Подмена страницы Web-сервера электронного магазина при помощи изменения записей в DNS-серверах либо в таблицах данных маршрутизаторов.
2. Перехват данных, которые передаются в системе электронной коммерции. (Наиболее опасен перехват информации о кредитной карте заказчика)

3. Человеческий фактор, выраженный в ненадежности сотрудников фирмы.
4. Атаки, влекущие за собой отказ работы сайтов организаций (в том числе вирусные).
5. Неумышленные действия обслуживающего персонала (ошибки, упущения и т. д.).

Также существуют факторы, от которых нельзя преодостеречься. Например, техногенные воздействия на систему (стихийные бедствия, пожары, крупномасштабные аварии и т. д.). В последнее время в электронной коммерции эффективно развиваются совершенно новые виды бизнеса, такие как Интернет вещей, 3-d печать, разнообразные формы взаимодействия по моделям C2C и M2M. Новые формы ведения бизнеса приводят к появлению и совершенно новых рисков в области информационной безопасности.

В итоге приходим к выводу, что создание абсолютной безопасности в сфере электронной коммерции невозможно, речь может идти только об достаточной безопасности. Существуют угрозы, влияние и действия которых почти всегда неизвестно. Для каждого предприятия выбирать следует свой набор средств безопасности в связи с разновидностью ведения бизнеса в сети Интернет.

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Сейтосманова Султание Рустемовна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

РЕКЛАМНЫЙ СПАМ И МЕТОДЫ БОРЬБЫ С НИМ

Спам – это массовая (до нескольких миллионов адресов) рассылка незапрошенной адресатами коммерческой или иной информации. От получения данной рассылки невозможно отказаться в будущем; она не требует предварительного согласия получателя и для ее совершения используются интернет-службы. Спам увеличивает риски для информационной безопасности.

Мошенничество, вымогательство, засорение почтовых ящиков, распространение вирусов и даже доведение человека до нервного срыва и многое другое осуществляется с помощью спама.

В апреле доля спама в глобальном почтовом трафике по подсчетам «Лаборатории Касперского» составила 71,1%, что на 7,6 пункта выше показателя за март [1].

По поводу методов борьбы со спамом проводятся множество дискуссий среди специалистов в области информационных технологий. Например, Билл Гейтс хотел ввести такую систему, по которой за рассылки взималась бы определенная сумма, а, учитывая, что злоумышленники отправляют их массово, они несли бы значительные финансовые потери [2].

Рассматривалась идея Е. Касперского [3], по которой каждому пользователю присваивается уникальный идентификатор, служащий для распознавания человека, занимающегося рассылкой спама.

Также предлагалось использовать электронную цифровую подпись — фактически очень длинный пароль, подобрать который практически невозможно. Таким образом, у одного человека существовала бы одна подпись-идентификатор, что исключало бы возможность последующего использования ее для рассылки спамов.

Существуют следующие рекомендуемые методы борьбы со спамом:

1. Нормативно-правовые методы, которые заключаются в наличии законов, регулирующих правомерность распространенной информации, предусматривающие законодательную ответственность за невыполнение требований законов.
2. Организационные методы:
   - разработка и распространение рекомендаций по использованию информационных систем;
   - распространение альтернативных спаму законных способов рекламной деятельности;
   - создание обществ по борьбе со спамом.
3. Программно-технические методы:
   - автоматическая фильтрация – сканирование сообщения с целью выявления спама;
   - чёрный список - перечень лиц, письма от которых не принимаются;
   - серые списки - перечень сервисов, письма от которых принимаются после повторной отправки (что не возможно для спам-программ).

В основном спам используется как достаточно эффективный вид рекламы. Рекламируется товар или услуга для накручивания счетчиков на сайте. Цель спама как вида рекламы — довести свою информацию до максимально возможного числа адресатов при минимальных издержках. Причем отправителей спама не волнует состав аудитории, для них главное — количество.

Проблема возрастания объемов спама в Интернете приобретает глобальный характер, что заставляет объединить участников рынка информационных технологий, исследовать опыт зарубежных стран. Не сдует надеяться, что данная проблема полностью исчезнет, риски от спама будут только возрастать [4]. Однако, интернет-провайдеры могут способствовать уменьшению ущерба от спама в результате специализированной подготовки штатных сотрудников, создания и распространения рекомендаций по использованию технологических фильтров.

Список использованных источников:

1. Касперский Е. В. Компьютерное зловредство / Е. В. Касперский. — СПб : Питер, 2007. — 208 с.
2. Ализар А.. Гейтс обещает уничтожить спам / А. Ализар // Веб планета [Электронный ресурс]. – Электрон. журн. – 2004. – 27 янв. – Режим доступа: http://www.sostav.ru/news/2004/01/27/8/, свободный. (Дата обращения: 10.01.2016).
3. Апрельский спам продемонстрировал рост / «Лаборатория Касперского» [Электронный ресурс]. — Режим доступа: http://kaspersky-cyberstat.com/rus/, ограниченный. (Дата обращения: 27.01.2016).
4. Королев О. Л. Модель оценки риска кибератаки для виртуального предприятия / О. Л. Королёв, С. В. Малков // Экономическая кибернетика. Международный научный журнал. — 2013. - № 1-3. — С. 80-85.

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Шеремет Ирина Юрьевна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ЗАДАЧА ВЫБОРА БЕЗОПАСНОГО ХОСТИНГ-ПРОВАЙДЕРА

На сегодняшний день можно констатировать, что фактически ни какой бизнес уже не может успешно функционировать без присутствия на просторах Сети Интернет. От качества и доступности Web-сайта предприятия в значительной мере зависит конкурентоспособность бизнеса. Web-сайт предприятия позволяет привлекать новых клиентов, рекламировать значительное количество разнообразных товаров, организовать возможность проведения on-line покупок.

Однако Web-сайт предприятия может стать источником проблем в развитии бизнеса. Клиенты предприятия, заходя на сайт могут подвергнуться «вирусной» атаке. Исследования проведенные SophosLab показали, что 80% Web-сайтов, в которых обнаружен вредоносный контент, были скомпрометированы внешним воздействием киберпреступников. Любой сайт может стать мишенью для атак такого типа, от крупнейшей мировой корпорации до регионального электронного представительства. В данном случае безопасность ваших клиентов и посетителей во многом зависит от выбора вами хостинг-провайдера.

Есть много факторов, которые необходимо рассмотреть при выборе организации в которой будет размещен Web-сайт, в том числе стоимость, пропускная способность, надежность и дополнительные услуги, но рассмотрим соображения связанные с безопасностью.

Хостинг-провайдер думает о безопасности Вашего сайта и предоставляемых услуг. Существует огромное разнообразие вариантов предоставления услуг хостинг-провайдеров, от поставщиков, которые дают вам только пространство на сервере и подключение и оставляют все вопросы, связанные с безопасностью вам, до тех, кто предлагает непрерывный мониторинг трафика, ежедневные сканирования вредоносных программ и другую разнообразную защиту, постоянно совершенствуют борьбу за информационную безопасность вашего Web-сайта.

Ключевой частью любой стратегии безопасности является план обработки нарушения безопасности: есть ли у провайдера процедуры, которые помогут временно ограничить доступ к вашему сайту, (доступ к «зараженному» сайту представляет опасность для ваших клиентов) и может ли хостинг-провайдер очистить и восстановить сайт и какое время это займет?

Важной ролью обеспечения любой платформы, на которой собственно и разворачивается Web-сайт, будь то сервер программы, или операционная система, является запуск обновлений и патчей связанных с безопасностью. В данном случае важно выбрать правильный баланс между эксплуатационной безопасностью и минимальным временем простоя.

Резервное копирование. Резервные копии являются необходимой процедурой предоставляемой провайдером безопасности. Есть две основных ситуации, в которых резервные копии могут играть ключевую роль: во-первых, в случае отказа оборудования у хостинг-провайдера и, во-вторых, в случае злонамеренного внедрения в ваш сайт. Зная есть ли резервное копирование данных и как долго займет процесс восстановления, можно оценить величину влияние инцидента на бизнес.

Самая важная составляющая вашего сайта, конечно, содержание. Как вы убедитесь, что ваш контент доставляется на страницы Web-сайта надежно, и что никто другой не может получить доступ к контенту. Протокол передачи файлов (FTP), хороший простой способ загрузить контента, но, к сожалению, не является безопасным. В идеале было бы предпочтительнее использование более безопасного метода, такого как SecureFTP (SFTP).

Часто доступ к загрузке контента зависит также от паролей модераторов сайта. Знать, кто загрузил контент также полезно для защите вашего сайта. Журнал доступа показывает, кто и как изменил сайт и эти данные могут помочь выявить какие-либо нарушения безопасности, связанные с действиями персонала ответственного за наполнение сайта.

В последние годы, различные виртуальные частные сети широко используются для предоставления доступа к сайту. Открытый характер Интернета требует обратить внимание на безопасность сетей хостинг-провайдера. Несанкционированный доступ к сети внешнего хакера или недобросовестного сотрудника хостинг-провайдера может вызвать повреждение или уничтожение конфиденциальных данных, что будет отрицательно влиять на ваш бизнес. Для предотвращения подобной ситуации хостинг-провайдером должны быть приняты такие меры предосторожности, которые позволят

гарантировать, что данные не доступны для тех, кому они не предназначены и что данные не могли бы быть изменены.

В бизнесе, один из самых важных приоритетов — максимизации прибыли. Неправильный выбор хостинг-провайдера может иметь негативное влияние на ваш доход. Так например, интернет-магазин Amazon за 40 минут простоя, потерял около 5 млн долларов. Потери для Вашего предприятия могут быть не так велики, но они по-прежнему потери дохода. Как говорится, "Вы получаете то, за что вы платите". В бизнесе, вы не можете позволить себе значительное время простоя Web-сайта. Ни один хостинг-провайдер не может гарантировать 100% время безотказной работы, но он должен предложить в среднем по крайней мере, 99% безотказной работы.

Для Web-сайт требующего имена пользователей и пароли необходимо защитить эти данные от перехвата. Использование HTTPS гарантирует, что все имена пользователей, пароли и другие конфиденциальные данные шифруются перед их отправкой через Интернет. Применение сертификата SSL с HTTPS также дает своим клиентам некоторые уверенностью, что вы думаете о безопасности, и может проверить подлинность вашего сайта для посетителей. В данной ситуации важнейшим становится возможность хостинг-провайдера соответствовать стандарту PCI DSS (Payment Card Industry Data Security Standard), предназначеному для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Решение о создании стандарта было вызвано резким увеличением числа инцидентов, связанных с утечкой данных о держателях платежных карт.

Требования стандарта PCI DSS распространяются на все компании, которые обрабатывают, хранят или передают данные о держателях платежных карт (банки, процессинговые центры, сервис-провайдеры, e-commerce и т.п.). Причем, требования относятся только к тем информационным системам компании, в которых обрабатывается или хранится информация о платежных картах, а также к системам, которые с ними взаимосвязаны.

Web-сайт вашего предприятия является окном, через которое глобальный мир смотрит на вас, на ваш бизнес и на ваше предприятие. Если Web-сайт представляет опасность для остального мира, то это будет плохо отражаться на вашем бизнесе. Ведение Web-сайт в безопасном режиме, с точки зрения информационной безопасности, не является тривиальной задачей. Выбор безопасного интернет-провайдера, получение помощи в рамках услуги хостинга, позволит значительно облегчить о бремя содержания Web-сайт в безопасном для владельцев и пользователей состоянии. Очень важно, чтоб хостинг-провайдер отслеживал вновь возникающие риски и оперативно овладевал инструментами для их нейтрализации.

УДК 004.9

Пенькова И. В.
профессор, д.э.н., профессор
Дытюк Л. И.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

E-MAIL-МАРКЕТИНГ

Email-маркетинг является одним из наиболее результативных инструментов продвижения. Он дает возможность непосредственного взаимодействия с возможными или имеющимися потребителями, результатом которого может быть выражен как в повышении лояльности клиентов к компании, так и в повышении новых и повторных продаж, возврате и удержании клиентов.

Эффективность E-mail маркетинга оценивается 4 основными показателями [1; 2]:

1. Open Rate – процент писем открытые потребителем.

Данный показатель имеет среднее значение 10%. В настоящее время наблюдается тенденция снижения показателя в связи с увеличением числа рекламных рассылок.

Производство и распределение товара (28,6%), искусство и мастерство (20,6%), безопасность и правоохранительная деятельность(19,3%) имеют самый большой показатель открытия писем. Бухгалтерский учет и финансы (6,6%), хобби (4,2%), подбор персонала (3,9%) имеют самый небольшой процент открытия писем.

2. Click Rate – процент писем, по которым клиенты сделали переход по ссылке.

Click-rate примерно составляет 1,9%-2% и наблюдается снижение данного показателя.

Безопасность и правоохранительная деятельность (7,5%), сельское хозяйство (3,5%), продукты питания, напитки и ИТ-услуги (3,5%) имеют самый большой показатель процента писем, по которым клиенты сделали переход по ссылке. Здравоохранение (0,8%), архитектура и строительство (0,7%), ресторан, бар и ночной клуб (0,5%) демонстрируют наименьший процент по показателю «Click rate».

3. Click Rate / Open Rate – процент конверсии или результативности рекламного сообщения.

Средний показатель «Click Rate / Open Rate» составляет 19%. Данный показатель не позволяет выявить тенденцию, поскольку он зависит от уникальности рекламных сообщений. Динамика показателя «Click Rate / Open Rate» отражается динамичным трендом. Понижение показателя приведет к поиску новых нестандартных решений привлечения покупателя, и к росту значения «Click Rate / Open Rate».

4. Bounce Rate – процент писем, не полученных потребителем в следствии спам-фильтров или по иным техническиим причинам. Доля недоставленных писем составляет от 0,4% до 4,4%.

Основываясь на приведенных данных, можно констатировать, что грамотное внедрение E-mail-маркетинга может достаточно быстро интенсифицировать трафик и создать конкурентные преимущества для фирмы, значительно расширяя целевую аудиторию.

Список литературы

1. Кот Д. E-mail маркетинг. Исчерпывающее руководство / Д. Кот // [Электронный ресурс]. – Режим доступа: http://www.litres.ru/static/trials/05/69/69/05696966.a4.pdf

2. E-mail marketing: полезные цифры для будущих рекламных кампаний / «POWERBRANDING» // [Электронный ресурс]. – Режим доступа: http://powerbranding.ru/trends/e-mail-marketing-poleznye-cifry-dlya-budushhix-reklamnyx-kampanij/

УДК 659.4

Пенькова Инесса Вячеславовна
д.э.н., профессор
Иванников Игорь Александрович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ ЗАЩИТА В ИНТЕРНЕТ-РЕКЛАМЕ

В современных условиях реклама распространяется как в реальном мире, так и в виртуальном, затрагивая все сферы деятельности, в том числе и те, которые осуществляются посредством Интернет. Интернет-реклама, представленная в глобальной сети, информирование потребителей о товарах, услугах или предприятии в сети Интернет адресованы массовому клиенту и имеют характер убеждения.

При сравнении типов Интернет–рекламы выявлено, что контекстная реклама целенаправлена на мгновенный результат, а баннерная может быть стимулирующей или имиджевой, что в свою очередь зависит от ее целей,.

Исследование особенностей восприятия рекламы, определено, что запоминается тот баннер, который является качественным в художественном и техническом плане. Однако статичный баннер с четким текстовым изложением содержания сайта тоже, имея низкий CTR, обычно неэффективен, так как он не создает положительного вприятия и не запоминается.

Обеспечение информационной безопасности при любом виде рекламы в интернет, заключается в том, чтобы:

- избавляться от информационного мусора;
- создавать надёжную защиту информации предприятия;
- блокировать проникновение мошенников информационную среду компании;
- не нести моральные и интеллектуальные издержки, связанные с уверенностью в сохранности важной информации на ПК;
- обеспечить защиту рекламного блока и сайта в целом от плагиата.

Как показывает практика, контент каждого популярного ресурса распространяется по сети, особенно в при высокой посещаемости. При этом особенно остро встает вопрос о защите информационной собственности от плагиата и о том, как отстоять права владельца, если их нарушают.

Случае обнаружения своих материалы на сторонних интернет-ресурсах, целесообразно предпринять следующие шаги:

- если владелец или разработчик пиратского сайта неизвестен, то существует возможность поиска сведений о нем или о провайдере ресурса, используя WhoIs-сервиса РосНИИРОС;
- после уточнения данных, следует написать плагиатору и администрации его хостинга письмо, потребовав удалить контент, принадлежащий другому собственнику;
- в случае игнорирования письма, надлежит заявить в правоохранительные органы, аргументируя свое обращение доказательствами авторства;
- и в последнюю очередь подается гражданский иск с требованиями материальной компенсации и закрытия сайта плагиатора.

Чтобы реклама в Интернете стала эффективным инструментом повышения рентабельности и прибыльности предприятия, целесообразно не только распространять о нем информацию, но и позаботиться об информационной защите контента официального сайта.

УДК 004.58

Пенькова Инесса Вячеславовна
д.э.н., профессор
Кислинг Эльвира Сергеевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА ИНТЕРЕСОВ ПРЕДПРИЯТИЙ С ПОМОЩЬЮ ПОИСКОВОЙ СИСТЕМЫ ЯНДЕКС

Сегодня, когда предприятия активно переводят свою деятельность в сеть Интернет, особенно актуален вопрос обеспечения безопасности бизнеса. Информационную защиту предприятия в сети можно выделить отдельным пунктом в системе информационной безопасности.

Бизнес, который ведёт политику интернет-маркетинга, одновременно защищает свой сайт от действий злоумышленников. Рассмотрим, каким образом могут нарушаться

интересы компаний, ведущих свою деятельность в сети Интернет, и какие инструменты Яндекс помогают защитить их.

Самая распространённая проблема для фирм, нарушающая авторские права – это копирование контента [1]. Маркетинговая политика фирм как правило направленна на выведение своего сайта на первые позиции в поисковой системе, для этого проводится ряд мероприятий направленный на оптимизацию сайта (SEO – search engine optimization). Первым делом seo-оптимизаторы добавляют в корень сайта файл robots.txt, он помогает ограничивать доступ к содержимому сайта и позволяет поисковой машине индексировать сайт и файл sitemaps.xml с информацией для поисковых систем о страницах сайта, которые следует индексировать. Только при условии наличия robots.txt сайт может быть индексирован поисковой системой. Так, если уникальная информация с сайта была скопирована и размещена на другом сайте, то на сайт будет наложен фильтр АГС, он запрещает индексацию интернет-ресурсов с неуникальным контентом, а, следовательно, и исключает сайт из списка ранжирования; или фильтр «ты последний» – накладывается на отдельную страницу со скопированным контентом. К сожалению, не всегда сайт, который был проиндексирован первым будет определяться поисковой системой как первоисточник, для этого Яндекс.Вебмастер предлагает сервис «Оригинальные тексты». Уникальный текст сначала загружается в Вебмастер, после чего добавляется на сайт.

Мошенническое действие (как правило со стороны конкурентов), которое значительно подрывает бюджет компании направленный на интернет-маркетинг – это так называемый кликфрод (англ. click fraud) или скликивание (может быть ручным или автоматизированным (кликботы)). В данном случае поисковой системой Яндекс предусмотрен фильтр за накрутку поведенческих факторов. К сожалению? избежать попадания под этот фильтр, даже если кликфорд является результатом действий конкурентов, невозможно. Основной признак попадания по фильтр – это резкое падение всех страниц в позициях, необходимо немедленно связаться со специалистами Яндекс и предупредить о возможных нарушениях со стороны недоброжелателей. Если к сайту подключена Яндекс.Метрика, то это позволит проводить мониторгинг и обнаруживать неоправданные изменения (например, резкое повышение количества посетителей).

Список литературы:

1. Неелова Н. Энциклопедия поискового продвижения [Электронный ресурс]. – Ingate, 2012. – 679 с.

УДК 004.9

Пенькова Инесса Вячеславовна
профессор, д.э.н., профессор
Кучинская Анна Александровна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ ЗАЩИТА ВИРТУАЛЬНЫХ ТОРГОВЫХ ПЛОЩАДОК

На сегодня все большее число пользователей обращается к услугам виртуальных торговых площадок и интернет-бизнеса в целом. Онлайновая торговая площадка является сайтом определенного рода, где заключаются сделки между покупателем и продавцом с проведением финансово-торговых транзакций [1-3]. С ростом востребованности такого бизнеса, растет и количество информационных угроз. Возможны следующие информационные угрозы участников виртуальных торговых площадок [2]:

- кража электронных подписей участников электронных торгов. При наличии доступа к контейнеру с закрытым ключом сертификата участника электронной торговой площадки, злоумышленник может совершать любые операции от лица владельца ключа;

- подмена подписываемого документа. Существуют программы, которые заменяют документы в момент подписания;
- доступ к списку участников аукциона. Если участники аукциона узнают друг о друге, то они смогут договариваться о ценах, что негативно скажется на принципе электронных торгов и принесет значительные убытки для заказчика;
- DDOS-атаки. Виртуальная торговая площадка должна обеспечивать постоянный доступ к серверу во время проведения торгов, так как нарушение непрерывности работы площадки ведет к срыву торгов, проводящихся в тот момент;
- взлом сайта площадки. Хакеры могут получить доступ к конфиденциальной информации и даже управлять ресурсом.

Существуют разнообразные программные продукты, обеспечивающие информационную защиту виртуальных торговых площадок.

Крипто-Экспресс предназначен для защиты данных от несанкционированного доступа, обеспечивает целостность передаваемой информации, с подтверждением подлинности ЭП (электронной подписи) и защищая электронный документ от фальсификации.

Архитектура Check Point позволяет успешно подстраивать защиту под специфические требования сетевой среды и бизнеса, способствуя предотвращению потери данных и предоставляя защиту от Интернет-угроз.

Symantec Endpoint Protection, являясь антивирусным решением, используется на любом компьютере с Windows, предназначено для защиты виртуальных и облачных дата-центров. Данный антивирус обеспечивает несколько слоев защиты за счет объединения технологий, позволяет защитить систему от тех вирусов, которых еще даже нет в базах.

Таким образом, следует отметить, что безопасность виртуальных торговых площадок в руках грамотных администраторов, использующих программные продукты, обеспечивает достаточно высокую степень информационной защиты.

Список литературы

1. Бойченко О. В. Информационная безопасность виртуального предприятия/ О. В. Бойченко, А. А. Кучинская// Теория и практика экономики и предпринимательства.: Гурзуф. -2015.- №23-25. – С. 179 – 180.
2. Угрозы безопасности клиентов электронных торговых площадок. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/blog/personal/aguryanov/29948.php
3. E-MARKETPLACES или виртуальные торговые площадки. // [Электронный ресурс]. – Режим доступа: http://www.i2r.ru/static/239/out_12476.shtml

УДК 336.7

Пенькова Инесса Вячеславовна
д.э.н., профессор
Мустафаев М. Р.
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Современная повседневная жизнь сложна без различных банковских операций, online- оплаты счетов или банковских карт. Такая ситуация стала результатом по причине общего распространения online-технологий, предоставляющих пользователям максимальный комфорт.

Электронную платежную систему называют системой онлайн расчетов, которые, как правило, хорошо защищены. Взлом счета обычно осуществляется потому, что клиенты сами разглашают конфиденциальную информацию о своем счете, по невнимательности храня пароль на видном месте, к примеру, в облаке с общим доступом.

В вопросе обеспечения безопасности электронной платежной системы должны быть реализованы следующие механизмы защиты:

- исключить возможность снятия средств со счета клиента третьими лицами
- предоставить плательщику законную возможность подтверждения совершения платежа, его назначение, перед третьим лицом (судом и т. д.)
- защита передаваемых средств с аккаунта от мошенников;
- исключение фальсификации квитанций;
- система должна быть устойчива к мошенникам;
- исключение вероятности попадания информации о клиенте посторонним лицам.

Безопасность электронных платежных систем гарантирует: защищенное интернет-соединение; клиентская защита (процедура входа в систему); техническая защита (привязка аккаунта к телефонному номеру).

По данным из исследований компаний Verison и Trustwave в 90-ти случая из 100 мошенники пытаются получить доступ к карточным данным. Электронная пластиковая карта выступает в роли носителя уникальной информации, по которой можно определить её владельца. На карту наносят логотип банка, фамилию и имя владельца, номер счета, а также срок действия карты. Это делается для идентификации владельца в случае выполнения каких либо операций со своим счетом при помощи банковской карты.

Безопасность электронной платежной системы зависит непосредственно от PIN-кода. Он может генерироваться банком исходя из номера счета при помощи алгоритма симметрического шифрования. В случае если вы забыли код, генерируется новый, но для этого, следуя инструкциям, нужно пройти процедуру восстановления контроля над своим счетом.

Также существую различные программно-технические способы защиты. К техническим средствам относят защиту сети электропитания, комбинированные устройства и системы. К программным средствам относят проверку паролей, антивирусную защиту базы данных, программы шифровки.

Технологии защиты платежных систем разнообразны. Они постоянно модернизируются и появляются новые. В первую очередь безопасность счета в электронной платежной системе зависит от клиента и его субъективного поведения.

УДК 336.7

Пенькова Инесса Вячеславовна
д.э.н., профессор
Пахомов Дмитрий Александрович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ БИРЖ

Электронной биржей считается таковая, что ведет торги с использованием информационной сети (ИС). Торговые операции проводятся пользователями (брокерами) с помощью абонентских систем, включенных в ИС.

Торговля на электронной бирже позволяет снизить временные затраты трейдеров и брокеров, повысить объемы оборота и увеличить количество заказов, увеличить скорость исполнения приказов и сократить операционные издержки.

Информационная безопасность служит для поддержания инфраструктуры от преднамеренных воздействий с целью нанесения ущерба владельцам и пользователям данной инфраструктуры.

Эта самая безопасность представляет собой состояние, при котором невозможен просмотр, изменение или удаление информации неуполномоченными лицами.

Защитой информации является совокупность манипуляций направленных на обеспечение целостности, конфиденциальности и доступности используемой информации для пользователей.

К основным характеристикам информационной зашиты относится:

- активность (защита информации с достаточной степенью целеустремленности);
- экономическая эффективность (отношение затрат на защиту системы к возможному ущербу);
- надежность (методы защиты должны перекрывать все возможные утечки информации).

Наиболее важным является непрерывное совершенствование системы информационной безопасности, а именно: постоянный контроль ее функционирования, обновление механизмов защиты, определение возможных каналов утечки из нее информации и несанкционированного доступа. Таким образом, обеспечение безопасности информации не может быть мероприятием одноразового типа.

Значимость имеет принцип комплексного использования полного арсенала доступных средств защиты во всех структурных элементах инфраструктуры производства и на каждом этапе технологического и технического цикла обработки данных. Потребность в комплексном характере защиты информации вызвана действиями злоумышленников.

Ключевыми условиями обеспечения защиты и безопасности информации представляются законность, взаимодействие с государственными правоохранительными органами, соблюдение баланса интересов личности и организации, достаточность, подготовка пользователей в части соблюдения установленных норм и правил конфиденциальности, высокий профессионализм сотрудников службы информационной безопасности и взаимная ответственность персонала и руководства.

Выполнение таких условий становится основой обеспечить требуемого уровня защиты данных и информационной безопасности. С позиции системного подхода для реализации приведенных принципов как процесс, так и сама система защиты информации должны отвечать определенной совокупности требований.

УДК 657.1.011.56

Пенькова Инесса Вячеславовна
профессор, д.э.н., профессор
Скрипник Евгений
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ИНТЕРНЕТ-МАГАЗИНОВ

Общий объем российской электронной коммерции составляет около 780 млрд. рублей. В России зарегистрировано около 40 тысяч Интернет-магазинов, из них реально функционируют около 30%.

Одной из основных проблем является организация доставки.

Покупатели на одном из самых знаменитых российских интернет-магазинов - Ozon.ru, в 77% случаев выбирают оплату наличными. Наиболее крупными сегментами интернет-магазинов по товарообороту являются Топ-5: 1) 150млрд рублей – электроника и бытовая техника . 2) 95 млрд. рублей – одежда и обувь; 3) 70 млрд. рублей – компьютеры и ноутбуки; 4) 38 млрд. рублей – автозапчасти; 5) 32 млрд. рублей - мобильные телефоны [1].

Успех в электронной торговле в основном, зависит от: выбора технологической платформы, конкурентоспособности продукта и наличия бизнес-процессов.

Продажи с сайта на 50% зависят от дизайна и юзабильности сайта магазина. Например, обеспечив пользователю возможность заказывать в «один» клик,

оптимизировать регистрацию и возможность оплачивать быстрыми денежными сервисами - обеспечит увеличение продаж

«Уровень» интернет-магазина определяется его общим денежным оборотом.

Для оформления интернет-магазина достаточно зарегистрировать ИП. Первая покупка через интернет состоялась в 1995 году – на сайте amazon была продана книга. Многие магазины используют социальные сети и службы фото и видео хостингов для рекламы и продвижения сайта (vk, youtube, instagram)

Одним из самым сложных в организации интернет-магазина представляется выбор поставщика товара. Желательно договариваться с теми поставщиками, где вы будете первым-вторым в цепочке поставок. Следует запросить образец товара и исполнять сделки, основываясь на заключении договоров.

Для того, чтобы составить выгодную стратегию продаж, необходимо знать цель и предпочтение потенциального клиента.

Для организации малого интернет-магазин достаточно собрать команду из веб-программиста, дизайнера, seo-оптимизатора и лидера проекта с соответствующим распределением функций.

Что бы максимально заинтересовать клиента, необходимо предъявить как можно больше информации о товаре. Она должна состоять из фотографии, технических характеристик, категории товара, код товара и торговой марки.

Рекомендуется создавать свои проекты, со своим внутренним кодом, так как «покупные» шаблоны зачастую отказывают в доступе к коду и изменить его можно, лишь купив ряд пакетов и лицензий.

Список литературы

1. Рынок интернет торговли в России в 2013 году / Аналитический обзор подразделения компании InSales (www.insales.ru). [Электронный ресурс]. – Режим доступа: http://www.bizhit.ru/InSales_2013_ecommerce.pdf.

УДК 004.056

Рыбников Андрей Михайлович
к.э.н., доцент
Гавриков Илья Владимирович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

АНАЛИЗ МЕХАНИЗМОВ ХЕШИРОВАНИЯ, ПРИМЕНЯЕМЫХ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ВЕБ-ПРИЛОЖЕНИЯХ НА ПРИМЕРЕ МУЛЬТИМЕДИЙНОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ «КУРС»

Аннотация. *Выбор оптимального алгоритма хеширования, с целью нейтрализации актуальных угроз и обеспечения информационной безопасности. Разработка Web-ресурса в полной мере удовлетворяющего требованиям безопасности.*

Ключевые слова: *Web-приложения, идентификация пользователя, аутентификация, авторизация, модели угроз, защита информации, хеш-функция, хеширование.*

В основе значительного количества веб-приложений сегодня лежит аутентификация пользователей. Она служит для разграничения полномочий в рамках приложения и защиты конфиденциальной информации от посторонних лиц[1]. Однако главной слабостью любой системы аутентификации является возможность взлома учётных записей пользователей. Эффективным механизмом обеспечения безопасной аутентификации является хеширование.

Существует множество различных криптографических хеш-функций, используемых сегодня в отрасли информационной безопасности. Среди самых популярных сегодня – алгоритмы MD5, SHA-1, SHA256, SHA512, RipeMD, WHIRLPOOL и bcrypt/scrypt.

Для обеспечения защиты мультимедийной обучающей системы «КУРС» от несанкционированного доступа был проведен анализ различных алгоритмов хеширования. Некоторые алгоритмы хеширования были исключены на стадии

планирования. Так, например алгоритм MD5 является устаревшим - ещё в 2004 году была показана его неустойчивость к коллизиям[2]. Также решено было отказаться от использования SHA-1, поскольку его безопасность находится под угрозой[3].

После анализа возможностей других алгоритмов было принято решение выбрать для хранения паролей хеш-функцию SHA512, как одну из самых безопасных и широко используемых на сегодня функцию.

Использование криптографических хеш-функций существенно затрудняет получение несанкционированного доступа к Web-ресурсам. Однако существует несколько видов атак, которые позволяют за достаточно короткое время восстановить пароли из простых хеш-кодов.

Наиболее опасный вид атак – это атаки с использованием радужных таблиц, содержащих миллиарды пар «пароль – хеш-сумма». Для решения данной проблемы необходимо использовать технику под названием «соление», которая делает невозможным использование радужных таблиц и таблиц поиска для взлома хеш-кодов. Соль — это строка случайных данных, подаваемая на вход хеш-функции вместе с исходными данными. В случае использования уникальной соли поиск паролей в таблице становится бессмысленным, и тогда единственный способ – перебор паролей по словарю или брутфорс с последующим их хешированием с уникальной солью и сравнением с имеющимся хеш-значением.

На практике это означает, что злоумышленнику понадобится значительно более мощная аппаратная база, ведь использование данной технологии нейтрализует преимущества атак с использованием «радужных таблиц» в скорости и эффективности.

Список литературы

1. Быков Д. В., Лукьянов В. С., Прохоров И. В., Скакунов А. В. Способы аутентификации и разграничения доступа к базам данных в сервис-ориентированных приложениях. // Известия Волгоградского государственного технического университета (№6, т. 6) – Волгоград, 2009 – С. 127
2. Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD — Университет Шаньдон / Китайская Академия Наук / Университет Шанхай Дзяотон, 2004
3. heise online. Hash-Funktion SHA-1 in Bedrängnis. – Режим доступа: http://www.heise.de/newsticker/meldung/Hash-Funktion-SHA-1-in-Bedraengnis-155135.html
4. Снегуров А. В., Чакрян В. Х. Анализ устойчивости ко взлому современных механизмов парольной защиты операционных систем. // Восточно-Европейский журнал передовых технологий (№10 / т. 2) – Харьков, 2011 – С. 27
5. Robert Morris, Ken Thompson. Password Security: A Case History. — Bell Laboratories, 1979.

УДК 004.056.5

Солдатов Максим Александрович
к.ф.-м.н., доцент
Запорожец Анна Андреевна
студентка 2 курса магистратуры
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

АНАЛИЗ ЭФФЕКТИВНОСТИ КОНТЕНТ-ФИЛЬТРАЦИИ В ДЕЯТЕЛЬНОСТИ КОМПАНИЙ

Контент-Фильтрация - это список контент-фильтров и услуг. Это программное обеспечение предназначено для управления доступностью содержимого читателям, в частности для фильтрации доступных через Интернет или электронную почту ресурсов. Ограничения могут устанавливаться на разных уровнях: государственная программа по блокировке во всей стране, блокировка интернет-провайдерами для пользователей, блокировка работодателями для работников, школы для учеников и студентов, библиотеки для её пользователей, родителей для детей, или просто само-фильтрация человека самому себе.

Контент-фильтр, или програ́мма ограниче́ния веб-контента (англ. Content-control software или web filtering software) — устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к

определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

Данная государственная программа закреплена нормативными документами:

- Федеральный закон от 25.07.2002 N 114-ФЗ "О противодействии экстремистской деятельности"
- Федеральный закон от 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с учетом №139-ФЗ от 28 июля 2012 года);

Контент-фильтр работает по статистическому принципу, то есть подсчитывает заранее определённые слова текста и определяет категорию, к которой относится содержимое сайта. Целью таких устройств или программ является ограничение доступа в Интернет для школ, предприятий, религиозных организаций и т. д. Чаще всего контент-фильтры используются для ограничения доступа для детей и подростков, в учебных заведениях, библиотеках и на рабочих местах в различных учреждениях.

Компания «Миранда-медиа», как интернет-провайдер предоставляет данную услугу с использованием Программного обеспечения UserGate Web Filter.

Эффективность данной услуги была оценена следующими характеристиками:

1. Ограничение доступа к запрещенным сайтам и отдельным страницам в сети Интернет, несовместимым с целями образования, которое осуществляется Компанией на основании законодательной базы.
2. При оказании разовой услуги «Черные/ Белые списки» Компания по заявлению Клиента с целью открытия доступа к сайтам (страницам сайтов), доступ к которым заблокирован в рамках Услуги, а также закрытием доступа к сайтам (страницам сайтов), доступ к которым не закрыт в рамках оказания Услуги.
3. Период предоставления Услуги – 24 часа 7 дней в неделю.
4. Доступность платформы СКФ составляет не менее 99,7% в месяц.
5. Регулярное обновление баз данных, запрещенных сайтов в сети Интернет.
6. Защита от фишинга, вида интернет-мошенничества, направленного на получение доступа к конфиденциальной информации, например, пароль доступа в интернет-банк. В структуре всех фишинговых атак более 34% приходится именно на финансовую сферу, более 32% на платежные системы.
7. Повышение эффективности работы компании. Социальные сети, сайты знакомств, форумы, online-игры — главные пожиратели рабочего времени и одна из причин снижения эффективности персонала. По оценкам аналитического агентства IDC, от 30 до 40 процентов интернет-активности офисных пользователей не имеет отношения к работе. А по данным Sextracker.com, 70% посещений сайтов с непристойным содержанием приходится именно на рабочее время.
8. Защита репутации компании – Клиента. Посещение сотрудниками с рабочего компьютера веб-ресурсов, размещающих незаконные, неэтичные или иные сомнительные материалы, может привести к серьезным репутационным и финансовым издержкам для предприятия.

В заключение можно сделать вывод, что в современных условиях работа компаний должна осуществляться с применением современных технологий защиты информации и ограничения доступа к Интернет-ресурсам. Одним из таких средств, позволяющих повысить эффективность работы компаний, является контент-фильтрация.

Список литературы:

1. Сайт Entensys (Общество с ограниченной ответственностью «еСЛ Девелопмент») // [Электронный ресурс]. – Режим доступа: http://www.litres.ru/static/trials/05/69/69/05696966.
2. Правовой ресурс «КонсультантПлюс» - Федеральный закон от 25.07.2002 N 114-ФЗ "О противодействии экстремистской деятельности"
   Федеральный закон от 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с учетом №139-ФЗ от 28 июля 2012 года);
3. Нормативная документация по регламентированию деятельности Компании при предоставлении услуги Контент-фильтрации.

УДК 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Шеремет Ирина Юрьевна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ РЫНКА M2M / IoT РЕШЕНИЙ

В настоящее время количество разнообразных материальных объектов подключенных к сети Интернет уже превышает количество людей пользующихся технологиями Интернет. Интернет Вещей (Internet of Things (IoT)) связывает много разнотипных устройств, передающих данные различным устройствам и приложениям заинтересованных пользователей. Модель (machine-to-machine) M2M объединяет телекоммуникационные и информационные технологии для автоматизации бизнеса.

Под рынком M2M сегодня подразумевается в большей степени рынок беспроводных мобильных устройств, использующих SIM-карты, основной целью которых является сбор и передача разнообразной информации без участия человека.

Согласно оценкам компании Berg Insight, в 2014 г. число беспроводных M2M-подключений в России выросло за год на 40%. По сравнению с общим количеством подключенных абонентских устройств это сравнительно небольшой количество [1].

Перспективный рынок M2M-устройств имеет значительный потенциал развития. Исследователями Cisco IBSG прогнозируется, что к 2020 году в мире будет эксплуатироваться около 50 млрд. различного рода устройств, реализующих «межмашинный» обмен. В настоящее время количество таких устройств не превышает нескольких миллионов. Пользователями M2M-сервисов чаще всего являются корпоративные клиенты. Представитель компании «Петер-Сервис» заявил о возможном размере российского рынка подобных услуг к 2017 году — 18,5 млн подключенных SIM-карт [2].

Для телекоммуникационных компаний, предоставляющих услуги сотовой связи отличием устройств M2M от абонентских устройств в обслуживании является гораздо большее количество абонентов с одной стороны и существенно меньший объем трафика в расчете на одно устройство с другой. При этом к оператору предъявляются большие требования относительно качественных характеристик.

К таким характеристикам относят доступность канала связи, задержка сигнала, его мощность и наиболее важная характеристика - уровень информационной безопасности.

Основной целью проектирования системы безопасности информационных технологий является предотвращение и снижение ущерба, который может быть нанесен участникам информационных отношений посредством нежелательного доступа к информации, воздействию на информацию, ее носители и на процессы ее обработки.

При этом система безопасности должна быть многоплановой и отражать различные угрозы, так как в M2M-приложениях зачастую используется стандартная операционная система и аналогичные протоколы и стандарты, что делает подключенные устройства уязвимыми для злоумышленников [3, с. 83].

M2M устройства непрерывно подключены к сети, что является отличной возможностью для проведения удаленной атаки

Специалисты, работающие в области безопасности, утверждают, что невозможно обеспечить безопасность на 100%. Но если говорить об устройствах функционирующих по модели M2M, то в этом случае необязательно обеспечивать такой же высокий уровень защиты, в частности, конфиденциальной информации, как, например, для продуктов банковской сферы [4].

Для обеспечения высокого уровня безопасности оптимальным вариантом является использование сертифицированной аутентификации и шифрования на основе протокола TLS /SSL. Для того, чтобы оператор связи мог контролировать безопасность своей инфраструктуры, необходимо использовать метод аутентификации с помощью общего

ключа или хеш-значения во время передачи смс-сообщения на мобильное устройство [3].

Современная политика информационной безопасности требует от всех сторон использующих M2M модель учитывать меры, ориентированные на снижение рисков. Современное состояние вопросов информационной безопасности для M2M приложений требует определения критериев для их оценки.

Любое предприятие стремится повысить свою экономическую эффективность. В настоящее время этого можно достигнуть путем переноса бизнес-процессов предприятия в «облако», доступ к которому предоставляется провайдером. Однако, такое решение повлечет за собой необходимость проведения значительных реформ в политике информационной безопасности. При переходе к использованию среды «облачного» сервиса необходимо учесть следующие положения, связанные с информационной безопасностью:

- разработать процедуры контроля обеспечения безопасности «облачным» провайдером с точки зрения выполнения требований информационной безопасности;
- разработать технические решения в рамках политики обеспечения безопасности информации в среде облачных вычислений;
- провести реформы на предприятии в связи с изменением правовых аспектов взаимодействия с «облачным» провайдером;
- провести анализ существующих угроз разработать их модели, оценить возможные юридические риски.

Сегодня рынок M2M / IoT состоит из слабо связанных между собою разрозненных задач, каждая из которых имеет решение своих специфических проблем. Наблюдается существенное изменение на уровне физического применения Интернета. Универсальной M2M / IoT системы не существует. В каждом отдельном случае существует необходимость разработки уникальной системы, которая будет оптимальной для бизнеса клиента, с собственной политикой информационной безопасности. Политика информационной безопасности должна быть, в первую очередь, обусловлена достижением баланса между удобством работы и необходимостью минимизации рисков, что при условиях повсеместного внедрения услуг модели M2M / IoT и прогнозируемым гигантским ростом использования этой модели является первостепенной задачей.

Список использованных источников:

1. Количество M2M-пользователей у операторов «большой тройки» [Электронный ресурс]. — Режим доступа: http://nag.ru/news/newsline/27412/kolichestvo-m2m-polzovateley-u-operatorov-bolshoy-troyki-.html, свободный. (Дата обращения: 10.01.2016).

2. «Петер-Сервис» внедрил M2M-платформу в «МегаФоне» / Сайт компании «PETER SERVICE» [Электронный ресурс] — Режим доступа: http://www.billing.ru/news/peter-servis-vnedril-m2m-platformu-v-megafone, свободный. (Дата обращения: 05.01.2016).

3. Королев О. Л. Модель оценки риска кибератаки для виртуального предприятия / О. Л. Королёв, С. В. Малков // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.

4. Безопасность M2M-коммуникаций / Михаэль Шульц //Еженедельник «IT Weekly», Михаэль Шульц [Электронный ресурс] — Режим доступа: http://www.it-weekly.ru/market/security/75934.html, свободный. (Дата обращения: 18.01.2016).

УДК 004.056

Рыбников Михаил Сергеевич
к.ф.-м.н., доцент
Гавриков Илья Владимирович
студент
ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ РЕШЕНИЙ MDM ДЛЯ ЗАЩИТЫ УСТРОЙСТВ В РАМКАХ КОНЦЕПЦИИ BYOD

Мобильные устройства стали необходимым средством ведения бизнеса. Но вместе с их востребованностью растёт и потребность в защите конфиденциальных данных. Стоит отметить, что в этом году рынок мобильных устройств впервые обогнал в своём

росте рынок персональных компьютеров. В связи с этим обстоятельством возникают проблемы с обеспечением безопасности обрабатываемых на устройствах конфиденциальных данных. Традиционные средства безопасности либо несовместимы с новыми аппаратными платформами, либо неспособны защитить информацию от нового класса атак и угроз. Одним из решений этих проблем являются системы MDM (mobile device management, англ. «управление мобильными устройствами»). В данной статье будет рассмотрено понятие MDM, функции систем MDM, их достоинства и недостатки.

С использованием мобильных устройств связаны совершенно новые векторы угроз, нехарактерные для персональных компьютеров. В общем их можно разбить на три группы: направленные на пользователей, на устройства и на сеть.

- Основными угрозами уровня пользователей являются потери и утечки данных, связанные с использованием сторонних приложений и облачных сервисов.
- Девайс-угрозы включают в себя использование уязвимостей мобильных операционных систем, непроверенные и злокачественные приложения, а также риск утраты или кражи устройства ввиду его миниатюрного форм-фактора.
- Сетевые угрозы в основном представлены атаками на устройства через перехват Wi-Fi траффика, атаки man-in-the-middle, небезопасные Wi-Fi точки доступа.

MDM (mobile device management) – набор технологий и средств, нацеленных на обеспечение безопасности мобильных устройств и защиту от угроз, описанных выше. MDM-решения всегда комплексны – помимо программных и аппаратных средств они включают в себя подходы к ведению бизнеса и политику по отношению к сотрудникам, направленные на обеспечение безопасности корпоративной информации.

- Угрозы со стороны пользовательских приложений устраняются посредством курирования каталога приложений, в который входят проверенные и безопасные корпоративные и сторонние приложения, а также созданием безопасной экосистемы на мобильном устройстве.
- Меры против девайс-угроз включают в себя жёсткое разделение личных и корпоративных данных, возможность удалённой блокировки доступа или удаления данных с устройства, настройку опций приватности и безопасности на уровне операционных систем, использование систем DLP (data leak prevention).
- Борьба с сетевыми угрозами ведётся посредством использования VPN на уровне приложений, регуляции доступа устройств к сети, а также использования строгой аутентификации с использованием сертификатов.

Основным недостатком модели MDM является практическая трудность создания такой системы, которая соответствовала бы всем требованиям к безопасности корпоративных данных и при этом была бы проста в настройке и использовании. Одной из основных причин этого является высокая фрагментация девайсов и разнообразие технологий и стандартов.

В ходе данного исследования было показано, что MDM-решения безусловно необходимы для обеспечения безопасности конфиденциальных корпоративных и личных данных в условиях современного рынка. Будущее модели MDM напрямую связано с развитием мобильного Интернета и облачных технологий. Возможные же проблемы безопасности исчезнут благодаря отсеиванию недобросовестных разработчиков и продавцов, а также развитию технологической базы.

Список литературы

1. Intel IT Center. Insights on the Current State of BYOD. Режим доступа: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf
2. Citrix Systems. Avoiding BYO Policy and Security Pitfalls. Режим доступа: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/avoiding-byo-policy-and-security-pitfalls.pdf
3. Contextis. MDM. The solution to BYOD? Режим доступа: http://www.contextis.com/documents/3/BYOD_in_the_Enterprise_-_Context_White_paper.pdf
4. MobileIron. Mobile Security Threats and Countermeasures. Режим доступа: https://www.mobileiron.com/sites/default/files/security/Mobile-Security-Threats-and-Countermeasures-WP-MKT-6361-V1.pdf

УДК 004.056

Белов Виктор Матвеевич
д.т.н., профессор
Крыжановская Ольга Александровна
студент
Плетнёв Павел Валерьевич
аспирант
ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики»
ФГБОУ ВО «Новосибирский государственный университет экономики и управления»
Новосибирск, Россия

ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ УГРОЗ В ОБЩЕЙ СХЕМЕ ОПРЕДЕЛЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Определение рисков информационной безопасности (ИБ) является начальным этапом создания системы защиты информации (СЗИ). В настоящее время существует большое количествометодик анализа рисков, несмотря на различия в подходах,как правило, общая схема оценки рисков выглядит следующим образом [1-3],:

1) определение характеристик объекта информатизации;
2) выявление уязвимостей с учётом принятых мер безопасности;
3) идентификация потенциальных угроз ИБ, на основе полученных данных;
4) определение вероятностей реализации угроз ИБ и потенциального ущерба;
5) оценка рисков ИБ;
6) оптимизация рисков ИБ;
7) документирование результатов проведённого анализа.

Поскольку обеспечение безопасности непрерывный процесс, необходимо осуществлять контроль эффективности принятых мер и подвергать результаты анализа регулярному пересмотру.

Получение вероятностей реализации угроз является одним из важнейших этапов оценки рисков информационной безопасности. Существующие методы оценки вероятностейможно разделить на три условных группы:качественные, количественные и комбинированные, каждая группа имеет свои достоинства и недостатки.

Количественные методы, основанные на использовании математических инструментов, позволяют получить более точную объективную оценку, однако требуют специальной подготовки от экспертов и проведения большого объёма предварительной работы, что отрицательно сказывается на временных затратах.

Качественные методы позволяют сформулировать разнообразные сценарии реализации угроз, оптимизировать процесс оценки вероятностей, но конечные результаты зачастую подвергаются субъективному влиянию экспертов.

Комбинированные методы сочетают в себе принципы качественной и количественной оценки: определение вероятностей угроз осуществляется на основе статистических данных и экспертного мнения.

Зачастую на практике эксперты сталкиваются с нехваткой статистических данных о частотах реализации угроз ИБ, в таком случае исходные данные дополняются субъективными оценками. Метод, основанный на сценарном подходе и факторном планировании эксперимента (ФПЭ), изложенный в работе [4, 5], позволяет решить данную проблему.

Планирование эксперимента – это процедура выбора числа и условий проведения опытов необходимых и достаточных для получения математической модели процесса [4, 5]. В основе данного метода лежит уравнение регрессии, описывающее зависимость между факторами и вероятностью реализации угрозы ИБ. Под факторами подразумевается уязвимость, создающая возможность для реализации угрозы.

Факторы оказывают влияние на вероятность реализации как самостоятельно, так и в совокупности, сценарный подход позволяет определить степень влияния каждого набора условий. Сценариям присваиваются уникальные значения по шкале от 0.00 до 1.00.

Количество сценариев зависит от количества факторов, в случае, когда рассматривается не более трёх факторов, проводят полный факторный эксперимент. При большем количестве экспериментов для упрощения работы экспертов осуществляется переход к дробному факторному эксперименту, опуская коэффициенты незначимых взаимодействий факторов.

В ходе планирования эксперимента составляется матрица планирования, содержащая сведения о сценариях реализации угроз.

Заключительным этапом является расчёт коэффициентов регрессии.

Алгоритм оценки вероятностей угроз ИБ представлен на рис.1.

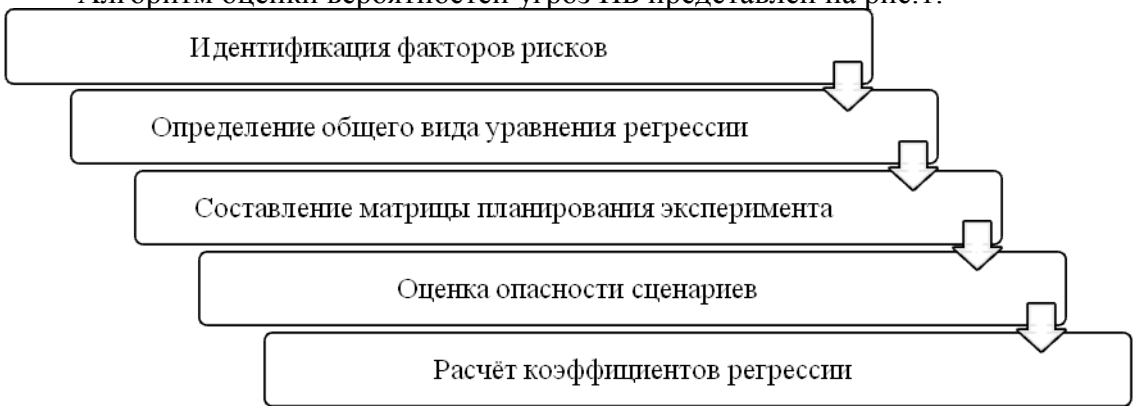


Рисунок 1 – Алгоритм оценки вероятностей угроз с использованием ФПЭ

В результате выполнения алгоритма получаем искомое уравнение регрессии. Таким образом, создаётся модель оценки вероятностей реализации угроз. Итоговые результаты позволяют судить о степени влияния каждого фактора на реализацию угрозы, и определить их взаимное влияние друг на друга.

Рассмотренная модель оценивания вероятностей реализации угроз ИБ с использованием ФПЭ позволяет учитывать сценарии реализации угроз и снизить субъективизм экспертов. Данный метод позволяет добавлять новые факторы, что упрощает процедуру переоценки рисков.

Литература

1. Плетнев П.В., Белов, В.М. Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. - 2011. - №3/1. - С. 221 - 223.
2. Белкин С. А., Белов В. М. Сравнительный анализ методов оценки угроз информационной безопасности // Доклады V1 Пленума СибРОУМО по образованию в области информационной безопасности и XV конференции, Томск – Иркутск, 9-13 июня 2014 г. Томск: В-Спектр, 2014. С. 188–194.
3. Белкин С. А., Белов В. М., Пивкин Е. Н. Об общей схеме оценки рисков информационной безопасности // Измерение, контроль, информатизация: материалы XV Международ. науч.-практ. конф. Барнаул: Изд-во Ал-тГТУ, 2014. С. 270–272.
4. Белкин С.А., Белов В.М., Пивкин Е.Н. Применение факторного планирования эксперимента для оценки вероятностей угроз информационной безопасности// Ползуновский вестник. - 2014. - №2. - С. 232 - 234.
5. Белкин С. А., Белов В. М. Оценка вероятности угрозы заражения компьютерным вирусом на основе факторного планирования эксперимента // Информационное противодействие угрозам терроризма. 2014. № 23. С. 55-61.

УДК 004.01

Бойченко Олег Валерьевич
д.т.н., профессор
Белименко Б. В.
студент 2 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСНОВЫ БЕЗОПАСНОСТИ АРЕНДЫ БИЗНЕС-ПРИЛОЖЕНИЙ

На сегодняшний день в России функционирует около сотни сервисов, предоставляющих возможность использования самого разнообразного программного обеспечения в удаленном режиме SaaS (оборот, клиентская база и т.д.) и количество этих сервисов постоянно растет. Однако анализ показывает, что при этом показатели рынка SaaS остаются довольно низкими, важнейшим сдерживающим фактором чего является проблема обеспечения информационной безопасности данных пользователя [1].

Практический опыт изучения современной деловой переписки указывает, что основным ее инструментом является электронная почта, где информация хранится и передается в открытом виде. Это создает проблему, связанную с тем, что провайдер может получить любую информацию по любым контактам, контрактам и передать ее, например, конкурентам.

Особый интерес с точки зрения проблемы защиты данных пользователей представляют Интернет-магазины. Так, в базах данных Интернет-магазинов собирается информация обо всех клиентах, их контактах, всех их заказах, товарных остатках на складах, уникальные описания и специально подготовленные пользователями изображения. Проблему обостряет то, что вся эта информация доступна провайдеру, имеющему возможность к злоупотреблениям. Проблемы безопасности SaaS-услуг ничуть не больше, чем проблемы безопасности стандартных хостинговых услуг, однако уровень этой безопасности устраивает огромное количество клиентов, что еще больше обостряет указанную проблему защиты персональных данных пользователей.

В случае жесткой конкурентной борьбы, конкуренты для получения информации пытаются «взломать» локальную сеть предприятия и/или ищут выходы на сотрудников и администраторов предприятия. При размещении информации у провайдера сотрудники и администраторы предприятия не только не имеют физической возможности получить доступ, но и не всегда известно, что эта информация вообще существует [2].

По нашему мнению, в такой ситуации, с целью решения проблем информационной безопасности при выборе поставщика услуг аренды бизнес-приложений необходимо следовать комплексу рекомендаций на основе следующей информации:

- история и репутация провайдера, квалификация персонала, клиенты;
- политика в области инфраструктуры, используемое серверное оборудование;
- системы внешней информационной безопасности (Firewall);
- сервиса параметров оказания услуг (SLA);
- наличие соглашения о конфиденциальности и его параметры (NDA);
- компетенции провайдера по предоставляемому программному обеспечению;
- служба технической поддержки с возможностью «эскалации» проблем;
- оформление документов в соответствии с законодательством РФ.

Использование указанных рекомендаций позволит создать условия для решения проблем защиты персональных данных пользователей при использовании бизнес-приложений в сетевых сервисах.

УДК 004.056.5

Бойченко Олег Валерьевич
д.т.н., профессор
Панченко Игорь Александрович
студент 1 курса магистратуры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

АНАЛИЗ ТЕНДЕНЦИЙ ИЗМЕНЕНИЯ В КАНАЛАХ УТЕЧЕК ИНФОРМАЦИИ

Цель исследования посвящена анализу тенденций изменения в каналах утечек информации, поскольку они играют основную роль в защите информации, являясь определяющим фактором информационной безопасности.

Каналами утечки информации из информационной системы являются методы и пути утечки, представляющие нежелательную цепочку носителей информации, один или несколько из которых могут быть правонарушителем или его специальной аппаратурой.

Для проведения анализа использован подход классификации каналов утечки информации из информационной системы, основанный на условиях их возникновения (случайные и умышленные), поскольку такое разделение уязвимостей защиты данных информационной системы наиболее ярко демонстрирует современное положение информационной безопасности автоматизированных систем управления предприятием.

Анализ тенденций изменения в каналах утечек информации проведен с 2010 года по 2014 год.

Так, по данным Infowatch за 2010 год было зарегистрировано 794 инцидента утечки информации, а так же число скомпрометированных записей почти 654 000 000.

По данным за 2014 год было зарегистрировано 1395 инцидента утечки информации, а так же число скомпрометированных записей составило почти 7,6 млрд.

На рис. 1. показано сравнительное соотношение случайных и умышленных утечек информации в 2010 и в 2014 году.

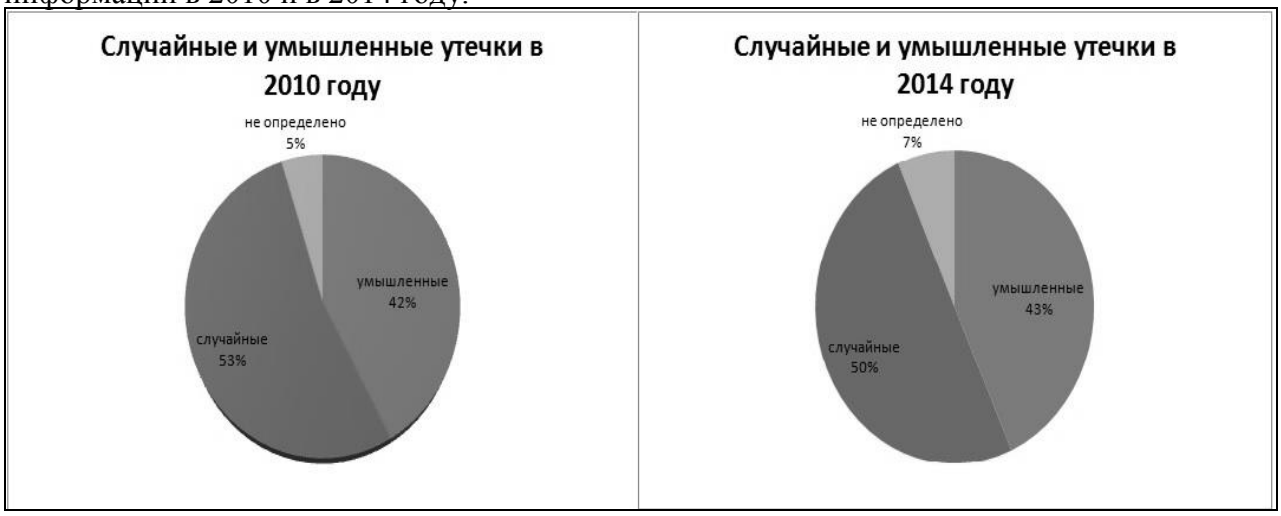


Рис. 1. Сравнительное соотношение утечек информации в 2010 и в 2014 гг.

На диаграммах отчетливо видно, что за выбранный период число умышленных и неопределенных утечек информации возрастает, что заставляет задуматься о характере таких утечек и способах защиты от подобных инцидентов.

Для более углубленного анализа и постановки задачи о необходимости усовершенствования подсистем защиты данных автоматизированных систем управления, проведено исследование сравнительной диаграммы с распределением каналов утечки информации по природе происхождения (Рис. 2).

Рис. 2. Сравнительное соотношение каналов утечки информации по природе происхождения в 2010 и в 2014 гг.

Рассмотрев диаграммы, можно сделать вывод о том, что количество умышленных утечек информации в нашей стране увеличилось и с каждым годом возрастает.

Причины такого положения дел кроются в аспектах связанных с бурным развитием информационных технологий, развитием электронного правительства, внедрением новейших технологий во все аппараты управления и обеспечение более доступной и быстрой работы с помощью Интернет.

Другой причиной является все большее вовлечение обычных пользователей к использованию услуг электронных платежей, интернет магазинов и прочих электронных сервисов, что так же влечет увеличение количества утечек информации.

Третьей причиной является несовершенство существующих систем защиты информации, поскольку любая система защиты данных проектируется и создается по необходимости построения барьера к изученным и установленным уязвимостям. Появление новых уязвимостей требует создания новой системы защиты, использования интеллектуальных (самообучающихся систем), способной противостоять любым проявлениям угроз к информационной системе.

Таким образом, проведенный анализ позволяет сделать вывод о необходимости создания новой эффективной системы защиты данных информационной системы управления (основанной на использовании интеллектуальных технологий), способной исключить потерю данных от утечек различной природы и условий их возникновения.

УДК 004.056.53

Бойченко Олег Валерьевич
д.т.н., профессор
Чачиев Владислав Русланович
студент 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РОЛЬ СМАРТ-КАРТ В СИСТЕМЕ КОРПОРАТИВНОЙ ИТ-БЕЗОПАСНОСТИ

Вопрос идентификации пользователя в системе контроля доступа крайне актуален. Любое предприятие, имеющее дело с коммерческой или государственной тайной должно внедрять методы шифрования и системы контроля и управления доступом для предотвращения действий злоумышленников по похищению, изменению или уничтожению данных. Смарт-карты вместе с системой двухфакторной авторизации значительно усложняют задачу злоумышленника по получению доступа к закрытым данным.

Целью работы является описание принципов работы смарт-карт на предприятии с закрытыми данным для выделения ключевых особенностей смарт-карт с шифрованием RSA и по ГОСТ Р 34.10-2012, применяемых в настоящее время на предприятиях и фирмах.

Смарт-карта – это специализированный для криптографии микропроцессор с повышенным уровнем безопасности. Доступ к памяти смарт-карты строго контролируется внутренним контроллером данных и не может быть считан без введения пин-кода.

Сегодня смарт-карты используются с целью однозначной идентификации пользователя или для аутентификации его действий в системах контроля управления доступом (СКУД) для выполнения следующих задач:

- контроль доступа к помещениям;
- авторизация пользователя во внутренней локальной вычислительной сети (ЛВС) предприятия;
- шифрование личных файлов, электронной почты, корпоративных файлов с ограниченным доступом;
- создание электронной цифровой подписи (ЭЦП) для удостоверения подлинности;
- авторизация и подпись документов;
- учет рабочего времени сотрудника.

Анализ современных способов авторизации в корпоративных системах позволяет выделить два способа для авторизации пользователя, такие как:

- пара «логин-пароль» (система – то, что знает только пользователь);
- система цифровых сертификатов, которые должны храниться только у авторизированного пользователя.

Использование смарт-карт позволяет дополнить оба способа и повысить надежность СКУД.

Следует отметить, что СКУД, построенные на принципе идентификации пользователя по логину и паролю достаточно широко распространены и много раз рассматривались в научных статьях. Однако сегодня наибольший интерес представляют ИТ-системы корпораций, построенные на базе сертификатов и использующие инфраструктуру публичных ключей (PKI).

Исследование показывает, что достичь строгой двухфакторной авторизации в корпоративных системах можно благодаря использованию криптографических смарт-карт и цифровых сертификатов.

Особенностью двухфакторной авторизации является строгое выполнение пользователем в процессе аутентификации требования по предоставлению двух признаков для однозначного определения персоны:

- смарт-карта (то, чем обладает только пользователь);
- PIN-код (информация, доступная только владельцу смарт-карты).

При этом, разрешение пользователю доступа к корпоративной ИС осуществляется только при совпадении этих признаков с базой данных пользователей системы управления. В иных случаях (после 3-х неуспешных попыток введения PIN-кода) производится автоматическое уведомление службы безопасности о возникновении проблемы с безопасностью на предприятии.

Анализ показывает, что принудительная двухфакторная авторизация является самым безопасным способом проверки подлинности пользователя в корпоративной среде для обеспечения необходимого уровня информационной безопасности автоматизированной управляющей системы.

Особого внимания требует вопрос внедрения смарт-карт на предприятии, в котором необходимо учесть несколько факторов:

1. Выбор адекватного алгоритма для построения PKI-системы (сегодня в РФ используется два стандарта – RSA-алгоритм, а также алгоритмы, описанные в стандарте ГОСТ Р 34.10-2012). Сравнивая указанные алгоритмы, следует отметить, что системы, использующие в своей основе алгоритм хеширования RSA, сейчас наиболее распространены среди систем СКУД в силу поддержки со стороны всех операционных

систем и многих корпоративных приложений. Эти системы относительно легко внедрять и поддерживать, эти системы рекомендуют для корпораций финансового сектора (биржи, банки, страховые компании). Характеризуя системы на базе ГОСТ Р 34.10-2012, следует указать, что они внедряются сложнее, однако обязательны для государственных учреждений и организаций (рекомендуется к применению в системах с максимально критической стоимостью потери данных). Потому этот алгоритм является сертифицированных в РФ, и теоретически является более стойким, нежели RSA.

2. Выбор необходимого программного обеспечения (ПО), которое будет выполнять роль «удостоверяющего центра» (УЦ) (УЦ является основным компонентом любой PKI-системы, выпускающим сертификаты открытых ключей и удостоверяющим их подлинность). Практика свидетельствует, что самым простым способом является использование УЦ, встроенного в Windows (Microsoft CA), поскольку Microsoft CA изначально рассчитан на работу с RSA-алгоритмом и может быть адаптирован и для работы по ГОСТу (например, при помощи решений компании КриптоПро). Помимо Microsoft CA существует много других УЦ, в том числе полностью ориентированных на работу только по ГОСТ Р 34.10-2012.

3. Выбор Card Management System (CMS) корпоративной информационной системы. CMS сопровождает сертификаты на протяжении всего их жизненного цикла: организует их выдачу, перевыпуск, отзыв. Поэтому к выбору CMS необходимо отнестись серьезно и основательно. CMS должна легко интегрироваться в информационную среду, поддерживать различные директории, удостоверяющие центры, модули безопасности (HSM), токены и смарт-карты. Желательна также возможность интеграции CMS и СКУД.

Таким образом, использование двухфакторной идентификации и авторизации на предприятиях с использованием смарт-карт в комплексе с перечнем рекомендаций их эффективного внедрения позволит создать условия для повышения эффективности функционирования корпоративной системы информационной безопасности.

УДК 303.064

Герасимова Светлана Васильевна
д.э.н, профессор
Гайдачева Анастасия Александровна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ТЕХНИКО-ПРАВОВЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЦИФРОВОЙ ПОДПИСИ

В наше время всё активнее стала использоваться электронная подпись, причём с каждым годом растёт количество стран в мире, где она внедряется, а также имеет и юридическую силу. Так, например, в Эстонской Республике широко используется система электронных подписей, путем введения программы ID-карт, которыми снабжены ¾ населения. Благодаря такой технологии значительно расширяется сфера электронного документооборота. В скором времени такая подпись будет применяться не только в бизнесе, но и в других сферах деятельности человека.

На сегодняшний день, проблема регулирования использования Электронной цифровой подписи (ЭЦП) в Российской Федерации становится наиболее актуальной. Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе [2, с. 9].

Электронно-цифровая подпись является аналогом обычной подписи и придаёт

правовую силу электронному документу. Имеет такую же силу, как и обычный документ, подписанный обычной ручкой, и скрепляется при помощи печати.

ЭЦП образуется вследствие криптографических процессов, которые заключаются в оригинальной очерёдности знаков, которые знает только владелец ключа. Такая подпись является очень надёжной и оригинальной, что способствует её использованию целым рядом организаций и предприятий.

С технической точки зрения ЭЦП подразумевает наличие открытого и закрытого ключей. Именно закрытый ключ и является электронной подписью, а открытый ключ определяет лицо, подписавшее документ и распространяются свободно, что нельзя сказать о закрытом ключе, который хранится у владельца. Конечно, подобрать закрытый ключ к открытому почти не возможно, и именно благодаря этому ЭЦП является более безопасной, чем обычная.

Взаимоотношения сторон, которые возникают в процессе применения данного вида подписи, требуют урегулирования со стороны закона. Так как такие отношения ещё слабо развиты в нашей стране, то они являются серьёзным преткновением для развития оборота документов в финансовой отрасли, государственном управлении, в частности, влияют на своевременность подачи информации гражданами страны, а также обмен документации с заграничными партнёрами.

На сегодняшний день огромное значение для цивилизованного развития такого сектора экономики как электронная коммерция играет и нормативно-правовая база. Начало этому было положено путем принятия Федерального закона от 10 января 2002 года №1-ФЗ «Об электронной цифровой подписи», но данный закон в 2011 г. утратил силу, а на смену ему пришел Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи". Основной целью принятия упомянутого акта было создание правовых условий для использования электронных документов в гражданско-правовой сфере [3]. Также в качестве одной из оставляющих нормативно-правовой базы в этой сфере регулирования можно назвать и Федеральную целевую программу "Электронная Россия (2002 -2010 годы)". Кроме того, Государственной Думой Российской Федерации был принят ряд законопроектов (N132742-4; N132754-4; N136018-4; N159016-4; N159631-4), призванных упорядочить отношения в сфере электронной коммерции и имеющих непосредственное влияние на развитие института электронной цифровой подписи.

Несмотря на то, что Федеральный закон "Об электронной цифровой подписи" N1-ФЗ от 10.01.2002 г. заложил правовые основы для функционирования информационных систем и применения ЭЦП в гражданском обороте, значительные пробелы в законодательном регулировании рассматриваемых отношений остаются главной причиной замедленного внедрения электронного документооборота в условиях рыночных отношений.

К актуальным проблемам, которые возникают при заключении договоров в системе электронного документооборота, можно отнести: затруднение в определении места заключения договора, сам факт заключения договора, а также сохранность и неизменность данных, содержащихся в договоре, конфиденциальность сведений, содержащихся в договоре [1].

На наш взгляд, авторы Закона об ЭЦП исходят из позиции, согласно которой вопросы применения цифровых подписей в корпоративных информационных системах не являются предметом жесткого законодательного регулирования. Законодатель сохраняет за корпоративными электронными системами свободу при определении порядка использования цифровых подписей, содержания информации в сертификатах ключей подписей, ведения реестра сертификатов ключей и иных вопросах. Привести на качественно новый уровень всю систему гражданско-правовых отношений поможет именно создание корпоративных информационных систем и вовлечение широкого круга предпринимателей в их деятельность.

Особенно, это актуально для организаций, осуществляющих деятельность в сфере компьютерных коммуникаций и электросвязи, поскольку именно здесь имеются и

высокий уровень применяемых технологий, и тесные связи между контрагентами, основанные на долгосрочных договорных отношениях, и публичность договорных отношений, вызывающая необходимость применения типовых форм гражданско-правовых договоров, и присутствие на рынке крупных корпоративных клиентов, способных создать развитые информационные системы и вывести отрасль связи на первое место в сфере развития новых форм документооборота [1].

Из всего вышесказанного можно сделать вывод, что лица, использующие ЭЦП, защищены от подделок документов, т.к. подобрать закрытый ключ к подписи потребуется очень много времени. Таким образом, основными преимуществами ЭП являются: экономия времени на совершение сделки, безопасность и надежность в использовании и хранении. Но, исходя из слабой законодательной базы в нашей стране, можно говорить об отсутствии доверия со стороны граждан РФ столь инновационным способам заключения сделок. Кроме этого, информация, которая содержится в электронных документах, требует определенной защиты от каких-либо несанкционированных изменений. Если же ужесточить законодательство в данной сфере, то на наш взгляд, в скором времени большинство позабудет что такое собственноручное заключение сделок.

Литература:

1. Батянов М.В., Лобачев В.В. Электронная цифровая подпись: проблемы правового применения: Материалы XI конференции представителей региональных научно-образовательных сетей RELARN-2004. - [Электронный ресурс]. - Режим доступа: www.ict.edu.ru/vconf/index.php.
2. Корелов С.В., Балыбердин А.В. Организация юридически значимого электронного документооборота с использованием электронной цифровой подписи: Методическое пособие / С.В. Корелов, А.В. Балыбердин; ННГУ. – Нижний Новгород, 2010. – 44 с.
3. Об электронной подписи : [федер. закон № 63-ФЗ от 6 апр. 2011 г.] // Рос. газ. – 2011. – 8 апр. – 18 полос.

УДК 004.056.5

Гончаров Сергей Михайлович
к.ф.-м.н., доцент
Боршевников Алексей Евгеньевич
ассистент
Кафедра информационной безопасности
ФГАОУ ВПО «Дальневосточный федеральный университет»
Владивосток, Россия

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вопросы обеспечения безопасности являются важными для многих областей современного общества. С развитием общества появляются новые технологии для решения указанных вопросов. Одним из путей решения является процедура биометрической аутентификации. Требования к уровню безопасности, обеспечиваемому такой процедурой, будут различаться в зависимости от объекта, на котором необходимо обеспечить аутентификацию пользователей. Для некоторых объектов необходимо использовать средства высоконадежной биометрической аутентификации.

Согласно ГОСТ Р 52633.0-2006 под высоконадежной биометрической аутентификацией понимается биометрическая аутентификация с приемлемой вероятностью ошибок первого рода (т.е. отказа системы аутентификации при обработки данных легитимного пользователя) и гарантированно малой вероятностью ошибок второго рода (т.е. срабатывания системы аутентификации при обработке данных злоумышленника), сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора [1].

Примером объектов, на которых необходимо обеспечить высокий уровень безопасности за счет использования процедуры высоконадежной биометрической аутентификации, могут выступить критически важные объекты [2].

Еще одним примером задачи, в которой необходимо обеспечить высокий уровень безопасности, является задача идентификации пользователя в процессе дистанционного обучения. Эта задача очень актуальна в дистанционном обучении. Перед дистанционным обучением ставится цель высококачественной подготовки специалистов без очного взаимодействия с преподавателем. Однако возникает проблема при проведении промежуточного или итогового контроля, заключающаяся в том, что необходимо с достаточно большой степенью достоверности убедиться в том, что данные виды контроля проходит обучающийся, который должен их проходить, а не третье лицо. Однако подобную технологию не целесообразно использовать для контроля написания работы в текущее время, так как это требует дополнительных усилий, которые будут отвлекать пользователя от сдачи аттестационной работы. Поэтому целесообразно применять для всего процесса прохождения аттестации двухфакторную аутентификацию. Можно предложить следующую схему аутентификации пользователей при прохождении аттестации при дистанционной форме обучения:

1. Пользователь регистрируется в системе и предоставляет необходимые биометрические данные;

2. Для начала прохождения аттестации пользователь проходит идентификацию с помощью средств высоконадежной биометрической аутентификации. В случае прохождения данной процедуры пользователю предоставляется доступ к заданиям. Если пользователь не прошел аутентификацию, то доступ не предоставляется;

3. Во время прохождения аттестации в случайный момент времени с помощью веб-камеры делается снимок изображения лица пользователя и сравнивается с предоставленными на этапе регистрации пользователем данными. В случае соответствия снятых данных предоставленным пользователь продолжает проходить аттестацию, в противном случае аттестация прерывается.

Опишем процедуру высоконадежной биометрической аутентификации. В общем случае процедура высоконадежной биометрической аутентификации заключается в восстановлении из нечетких биометрических данных с использованием специально сгенерированных данных некоторой фиксированной битовой строки (криптографический ключ, код доступа, пароль). Основным преимуществом систем, основанных на описанном методе, является то, что вся аутентифицирующая информация не хранится в открытом виде, а хранится в виде некоторого хешированного значения. Это уменьшает размеры базы данных, используемой для аутентификации, а также позволяет обезопасить биометрические данные от компрометации.

В настоящий момент в мире на практике используются два подхода к реализации технологии высоконадежной биометрической аутентификации:

1. Подход, основанный на использовании "нечетких" контейнеров и "нечеткой" математики;

2. Подход, основанный на использовании аппарата больших и сверхбольших нейронных сетей (нейросетевые преобразователи "Биометрия - код доступа").

По данным открытых источников характеристики (вероятность ошибки первого рода, вероятность ошибки второго рода) нейросетевых преобразователей "Биометрия - код доступа" выше, чем характеристики биометрических систем, использующих "нечеткие" экстракторы [2]. Преимуществом "нечетких" экстракторов является их возможность использования для большинства видов биометрических характеристик, тогда как для нейросетевых преобразователей подробно описаны и изучены системы на основе рукописного почерка.

Одним из перспективных направлений исследований является разработка технологии высоконадежной биометрической аутентификации на основе электроэнцефалограммы (ЭЭГ). Использование ЭЭГ в качестве биометрической характеристики имеет следующее преимущество - ЭЭГ сложно снять незаметно для

пользователя, а также ее трудно подделать в силу сложности самой природы сигнала ЭЭГ.

В работе [3] в качестве биометрической характеристики, используемой в нейросетевом преобразователе, брался сигнал ЭЭГ под воздействием внешней зрительной стимуляции. Предварительные расчеты дали вероятность ошибки 2-го рода ниже, чем 10^{-12}.

Отдельный интерес представляют системы без внешней стимуляции. Проводились исследования на основе ЭЭГ, возникающей при специфическом движении глаз с закрытыми веками. Для выделения потенциала движения мышц глаз было решено провести следующий эксперимент. Для упрощения проведения эксперимента использовалась звуковая стимуляция метрономом, с интервалом 2 секунды. Запись данных производилась в течение 8 секунд. На каждый удар метронома испытуемый производил одно из движений алфавита 1 (движение влево, вправо, вверх, вниз) или алфавита 2 (движение влево, вправо, влево-вправо, вверх, вниз, вверх-вниз, по кругу). Последовательность движений составляет пароль.

Опишем структуру и принцип работы нейросетевого преобразователя "Биометрия - код доступа". Для обработки полученных данных в качестве структуры преобразователя выбрана двухслойная нейронная сеть с сигмоидальными передаточными функциями. Для обучения выбрана стандартная процедура обучения нейросетевых преобразователей "Биометрия - код доступа", описанная в стандарте ГОСТ Р 52633.5-2011 [4]. Для обучения необходимо сформировать базу электроэнцефалограмм при воздействии стимуляции образов "Чужой", т.е. образов злоумышленника, для которых нейронная сеть будет выдавать случайный криптографический ключ. Данную базу можно использовать для последующих процессов обучения преобразователя. Также необходимо сформировать базу электроэнцефалограмм образов "Свой" - пользователя, который будет считаться легитимным. Данную базу необходимо удалить сразу после обучения преобразователя, в целях предотвращения её кражи и использования для компрометации секретного ключа. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети:

$$\overline{w_i} = \{w_{ij}\}, 1 \le i \le I, 1 \le j \le J,$$
$$\overline{W} = \{W_k\}, 1 \le k \le K,$$

где $\overline{w_i}$ – вектор весовых коэффициентов первого слоя нейронной сети, соответствующий вектору биометрических данных $\overline{a_i}$; $\overline{W}$ – вектор весовых коэффициентов второго слоя нейронной сети; K – количество нейронов первого слоя.

Нейроны первого и второго слоя сходны по строению, но имеют различие в обрабатываемых данных и получаемых результатах. Для описания работы первого слоя введем следующую величину:

$$v_i = \overline{a_i} \cdot \overline{w_i}, 1 \le i \le I.$$

Это нормированная величина, которая подается на входы сумматоров с электрода i. Составим вектор таких значений:

$$\overline{v} = \{v_i\}, 1 \le i \le I.$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,k} = \overline{v} \cdot \overline{net_k},$$
$$\overline{net_k} = \{\Delta_i\}, 1 \le i \le I,$$
$$y_{1,k} = \frac{2}{1+e^{x_{1,k}}} - 1,$$
$$t_k = f_1(y_{1,k}) = \begin{cases} 1, y_{1,k} \ge 0 \\ -1, y_{1,k} < 0 \end{cases}, 1 \le k \le K,$$

где $x_{1,k}$ – это результат работы сумматора нейрона k первого слоя; $\overline{net}_k$ - вектор связей нейрона k; Δ_i – коэффициент использования данных электрода i в нейроне. Если электрод используется в данном нейроне, то $\Delta_i = 1$ и $\Delta_i = 0$ в противном случае; $y_{1,k}$ – передаточная функция первого слоя нейронной сети; $\mathrm{f}_1(y_{1,k})$ – решающее правило для нейрона первого слоя.

Используемые в сумматорах нейрона вектора нормированных биометрических данных определяются следующим образом. В любом сумматоре обязательно используется один из нескольких векторов, соответствующих векторам данных, характеризующим наиболее сильный потенциал движения глаз. Для оставшихся входов сумматора используются не использованные вектора нормированных биометрических данных.

Каждый нейрон второго слоя можно описать следующим образом:

$$x_{2,l} = \sum_{k=1}^{K} W_k t_k \Delta_l \ , 1 \le k \le K \ ,$$

$$y_{2,l} = \frac{2}{1 + e^{x_{2,l}}} - 1,$$

$$k_l = \mathrm{f}_2(y_{2,l}) = \begin{cases} 1, y_{2,l} \ge 0 \\ 0, y_{2,l} < 0 \end{cases}, 1 \le l \le L \ ,$$

где $x_{2,l}$ – это результат работы сумматора нейрона второго слоя; Δ_l – коэффициент использования компонента t_k в нейроне. Если t_k используется в данном нейроне, то $\Delta_l = 1$ и $\Delta_l = 0$ в противном случае; $y_{2,l}$ – передаточная функция второго слоя нейронной сети; $\mathrm{f}_2(y_{2,l})$ – решающее правило для нейрона второго слоя; L - длина восстанавливаемого криптографического ключа.

Используемые в сумматорах нейрона выходы первого слоя определяются согласно процедуре, описанной в ГОСТ Р 52633.5-2011 [4].

Результат работы каждого нейрона второго слоя k_l является битом восстанавливаемого секретного криптографического ключа.

Во всех опытах по восстановлению ключа легитимным пользователем вырабатываемый секретный ключ размером 256 бит всегда совпадал с истинным. Даже в случае, когда злоумышленник угадывает "мысленный пароль", минимальное расстояние Хэмминга (количество ошибок) до ключа легитимного пользователя было равно 15. При генерации злоумышленником ошибочного «мысленного пароля» усредненное расстояние Хэмминга до истинного ключа заметно выше.

Результаты исследования по получению злоумышленником секретного ключа размером 256 бит с помощью нейросетевого преобразователя при условиях знания пароля приведены в таблице 1. H_7 - расстояние Хэмминга при использовании алфавита «мысленных образов», состоящего из 7 символов.

Номер пользователя	H_7
1	136
2	138
3	47
4	20
5	143
6	15
7	88
8	50
9	144

Таблица 1. Расстояние Хэмминга до секретного ключа пользователя в случае знания злоумышленником пароля

Полученные результаты показывают возможность эффективного использования технологии высоконадежной биометрической аутентификации в задачах по обеспечению при обеспечении безопасности.

Список литературы

1. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации: ГОСТ Р 52633.0-2006. – Введен впервые; Введ. 27.12.2006. – М.: Стандартинформ, 2007. – 25 с.

2. Гончаров С.М. Использование технологий высоконадежной биометрической аутентификации в критически важных объектах / С.М. Гончаров, А.Е. Боршевников // Информационная безопасность регионов. – Саратов: Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2015. – № 4 (21). – С. 18–23.

3. Гончаров С.М. Построение нейросетевого преобразователя "Биометрия - код доступа" на основе параметров визуального вызванного потенциала электроэнцефалограммы / С.М. Гончаров, А.Е. Боршевников // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. – Томск: Изд-во ТУСУР, 2014. – № 2. – С. 51–55.

4. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия - код доступа: ГОСТ Р 52633.5-2011. – Введен впервые; Введ. 01.12.2011. – М.: Стандартинформ, 2012. – 20 с.

УДК 621.391

Гончарова Оксана Николаевна
д.п.н., профессор
Шпилевой Евгений Владимирович
магистрант
Таврическая академия, факультет математики и информатики
Крымский федеральный университет имени В.И. Вернадского
Республика Крым, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном глобальном мире проблема информационной безопасности имеет решающее значение. Данным вопросом занимаются на самых различных уровнях, начиная с небольших предприятий и заканчивая государствами и мировыми корпорациями. Уже к концу XX века были реализованы случаи ведения информационных атак в военных конфликтах. А согласно данным зарубежных правоохранительных органов, для примера, в той же Германии с использованием компьютера ежегодно похищается до 2 млрд евро.

Если рассматривать безопасность информационных систем, то следует разделять две области: сетевую безопасность и безопасность компьютера. Вторая задача, в чем-то является более простой, ведь речь идет об автономной системе. Она сводится к тому, чтобы предотвратить незаконный доступ к данным на конкретном месте, чего можно добиться установкой охранных систем, идентификацией пользователя по отпечаткам пальцев, сетчатке глаза и т.п.

Компьютер же, который работает в сети, никоим образом нельзя изолировать от мира, ведь он и должен взаимодействовать с другими компьютерами, которые могут находиться на другом конце мира. Суть его работы и состоит в том, чтобы чужие пользователи получали доступ к этому устройству и его данным. И организация безопасности заключается в том, чтобы это проникновение было контролируемым. Каждому пользователю необходимо выделить лишь строго определенный доступ к информации или внешним устройствам. Однако и тут есть слабые места, связанные с тем, что злоумышленник может получить доступ к чужому паролю. Кроме того, сети подвержены и другого рода опасностям – перехвату и анализу сообщений, которые передаются по сети, созданию «ложного» трафика.

Безопасная информационная система характеризуется тремя свойствами: конфиденциальностью (секретные данные должны быть доступны только авторизованным пользователям), доступностью (авторизованные пользователи всегда должны иметь возможность получить доступ к данным) и целостностью

(неавторизованные пользователи не имеют возможности что-либо изменять, разрушать или создавать новые данные).

Угрозы информационной безопасности с каждым годом становятся всё сложнее, хакеры и киберпреступники разрабатывают всё новые и новые приемы, проводят всё более изощренные атаки с целью взлома систем и кражи данных. Это заставляет искать новые решения и стратегии для противодействия их незаконным действиям. И эта сфера является крайне перспективной для дальнейших исследований и открытий.

УДК 004.056

Иванов Сергей Викторович
к.ф.-м.н., доцент
Кравцов Игорь Олегович
студент 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Деньги являются неотъемлемым атрибутом нашей жизни. И очень часто нам необходимо проводить обмен этими материальными ценностями. Это обусловлено нашей историей: начав с бартера, пройдя введение купюр, платёжных поручений и чеков система платежей видоизменялась, но никак не меняла уровень своей значимости. Самый современный метод проведения платежей – электронная коммерция. Несомненно он наиболее удобный и быстрый, но что можно сказать о его безопасности? Насколько защищёнными являются платежи, проводимые в сети «Интернет»?

Сторонами электронных платежей являются плательщик и получатель. Целью их проведения будет служить перевод денежных средств плательщиком получателю. В электронных системах такой платёж сопровождается протоколом электронного платежа. Также необходимо наличие финансового института, которым может выступать банк и который будет сопоставлять и проверять данные протоколов с перемещениями реальных средств. Банки могут выполнять две роли: эмитента, т.е. взаимодействующего с плательщиком; и эквайрера – работающего с получателем. Помимо этого, в платежной системе необходимо наличие арбитра для разрешения возникающих споров.

Естественно, использование Интернета в столь конфиденциальном и важном процессе вызывает у многих недоверие и большие опасения. Поэтому наличие хорошей системы безопасности в электронных платежах является необходимой частью их архитектуры. В связи с этим можно выделить следующие требования к безопасности электронных платежей:

- исключение возможности списания средств с аккаунта плательщика третьими лицами;
- обеспечение возможности официального подтверждения совершения платежа плательщиком и факта его получения получателем перед третьим лицом;
- обеспечение гарантий, что перемещаемая с аккаунта сумма не будет украдена в момент передачи и попадет точно по назначению;
- исключение возможностей подделки квитанций эмитента пользователям;
- разрешение спорных вопросов между пользователями и эмитентом исключительно электронным образом с помощью цифровой подписи;
- возможность разрешения спорных вопросов между пользователями без участия финансового института; система в целом должна быть устойчива к мошенническим действиям, в том числе и в случае форс-мажорных обстоятельств.

К обеспечению защиты электронных платежей необходимо подходить комплексно, недостаточно иметь лишь SSL сертификат на сайте. На уровне клиентской защиты необходимо наличие:

- логин и пароль доступа для входа в систему, который проходит тестирование на сложность (или выдается для каждого сеанса);
- комбинация номера банковской карты, срока действия, имени держателя карты, CVV/CVC кодов;
- возможность создания виртуальной карты, дублирующей основную, для проведения интернет-платежей;

Техническая защита проведения платежей должна обеспечиваться путём:

- привязки платежного сервиса к фиксированному IP-адресу и телефонному номеру клиента;
- осуществления клиентского доступа в систему по зашифрованному протоколу HTTPS/SSL;
- возможности использования виртуальной клавиатуры для набора данных идентификации, для обеспечения противодействию перехвата личных данных;
- разделения каналов формирования и авторизации транзакций:
- авторизации транзакций осуществляемых через специальный код, который при совершении платежа клиент получает от системы на свой мобильный телефон (случайная комбинация букв и цифр, действующая только в течение нескольких минут).

Приведенные условия и требования являются лишь частью общего пакета безопасности. Методы и подходы к защите электронных платежей проходят проыерку на прочность каждый день и постоянно совершенствуются.

Список литературы

1. Бирюков А.А. Информационная безопасность. Защита и нападение[текст]: учебник/ Бирюков А.А. – М.:ДМК Пресс, 2012. – 474 с.
2. Кочергин Д.А. Электронные деньги[текст]: учеб.пособие/ Д.А.Кочергин. – М.:Маркет ДС; ЦИПСиР, 2011. – 424 с.
3. Лугачев М.И. Экономическая информатика. Введение в экономический анализ информационных систем[текст]: учебник/ Лугачев М.И., Анно Е.И., Когаловский М.Р., Липунцов Ю.П., Скрипкин К.Г., Смирнов С.Н., Смирнова Е.Е. – М.: Проспект, 2016. – 805 с.
4. Прохоров А.А. Платежные системы в Интернет / А.А. Прохоров, О. А. Горнев // [Электронный ресурс] / Режим доступа: http://compress.ru/article.aspx?id=9848&iid=413

УДК 330

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Кушнир Дмитрий Алексеевич
студент
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИЯХ КУРОРТНОЙ СФЕРЫ

Информационная безопасность — один из важнейших приоритетов как информатизированной экономики общества, так и для отдельных предприятий в частности. Этот термин можно определить как такое состояние информационных ресурсов субъекта, при котором они защищены от непредусмотренных и незаконных действий как извне, так и изнутри. При внедрении на предприятия различных программных компонентов увеличивается необходимость в информационной безопасности. Задача их руководства при этом — минимизировать риски насколько это возможно. Для Республики Крым курортно-санаторная сфера — перспективное на данный момент направление, развитие которого приведёт к общей экономической

развитости региона.

Для автоматизации работы эти предприятия внедряют специализированные программные средства, в частности Корпоративные Информационные Системы (КИС).

Эксперты выделяют такие виды угроз информационной безопасности предприятия:

1) Действия, совершаемые сотрудниками. В настоящее время сотрудники санаторно-курортной отрасли активно используют в своей профессиональной деятельности разнообразные КИС, например такие как «1С-Бухгалтерия», при помощи которых они оперируют важными данными. При этом могут быть введены неверные данные, или выполнены неверные действия. Это может быть совершено как умышленно, так и по неосторожности;

2) Угрозы извне представляют меньшую опасность, однако и они могут причинить вред. Веб-сайт санатория либо пансионата, предоставляющий информацию о нём и дающий возможность приобрести его продукцию, может быть подвергнут злоумышленниками DoS-атаке. Такая атака, направленная на вывод из строя серверов, на которых располагается сайт, делает невозможным использование сайта. Целью такой атаки может быть шантаж или давление на конкурента в бизнесе;

3) Компьютерные вирусы представляют собой опасность для любого современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Такие вредоносные программы могут нанести непоправимый вред деятельности фирмы, захватив контроль над её данными;

4) Спам. Часто спам — не только отвлекающий фактор для работников, пользующихся компьютером, но и главный источник вирусов из глобальной сети. Отделение спама от обычных писем является сложным процессом и в нём тоже можно не избежать ошибок, потеряв в результате важное письмо, определённое как спам;

5) Естественные угрозы. Опасность также представляют различные естественные факторы: пожары, сбои в подаче электроэнергии и другие.

Все эти факторы угрожают информационной безопасности курортных предприятий, наиболее важные из них это: фактор компьютерных вирусов, так как эта угроза имеет глобальный характер и угрожает абсолютно каждому пользователю интернета, и фактор естественных угроз, готовым к которым должно быть каждое предприятие.

Для обеспечения информационной безопасности нужно решить такие задачи как: обеспечение защищённого хранения данных; защита каналов связи; разграничение прав доступа к различной информации; обеспечение резервного копирования.

Стоит сказать, что достижение информационной безопасности — не единоразовое действие, а постоянный процесс, в котором защитные средства должны адекватно соответствовать угрозам, что является одним из важнейших ключей к процветанию бизнеса.

УДК 338 : 004.056.5

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Таштанова Лидия Лативицевна
студентка
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНОЛОГИЯХ АДДИТИВНОГО ПРОИЗВОДСТВА

3D-печать, или технологии аддитивного производства – это процесс воссоздания объемных объектов практически любой формы из 3D-модели или другого электронного ресурса информации. Эта информация, которая храниться в цифровом формате, как и остальные виды цифровых данных, уязвима и может быть подвержена кибер-пиратству и нарушению прав интеллектуальной собственности.

Вопрос об актуальности данной темы встает, когда появляется угроза нарушения не только авторских прав на частные модели конструкций, а прежде всего при угрозе интеллектуальной собственности предприятий.

Технологии аддитивного производства предоставляют предприятиям возможности, не только связанные с преимуществами данных технологий по сравнению с традиционными способами создания моделей и прототипов, но и по повышению эффективности производства в целом. Получение деталей для производства или отправка изделия покупателю, предоставление его через сайты в корне меняет логистическую цепь производства. Снижаются издержки производства, устраняется необходимость в содержании складских помещений, доставка конечному потребителю продукции становится практически беззатратным процессом.

С внедрением технологий аддитивного производства на мировом рынке, предприятия начнут подключать различные новые методы и устройства в цепи производства и логистики, которые потребуют значительные объемы информационных ресурсов для оперативного управления и поддержания процесса производства. Данная информация будет содержаться в коммерческой тайне, но так как речь идет о 3D-печати, и подразумеваемая информации содержится в цифровом формате, то и информационная безопасность на предприятии принимает более серьезные масштабы. Если рассмотреть для примера предприятие, занимающиеся производством военного оборудования по госзаказу, то информационная безопасность такого предприятия переходит в рамки национальной безопасности.

Внедрение технологий аддитивного производства приведет к увеличению роли информационных технологий в целом и, как следствие, значимости информационной безопасности.

Можно выделить следующие основные проблемы, с которыми технологиям аддитивного производства придется столкнуться в будущем:

1) Нарушение прав интеллектуальной собственности (в частности авторское и патентное право);

2) Появление на рынке некачественной поддельной продукции;

3) Установление авторства на модель, находящуюся в открытом доступе и привлечение к ответственности за нарушения прав на интеллектуальную собственность.

Создать 3D-модель можно двумя основными способами: с помощью систем автоматизированного проектирования и при помощи 3D-сканера. В первом случае, создав модель и разместив ее в открытом доступе, автор практически теряет контроль над ее будущим. Любой пользователь того Интернет-ресурса, на котором была размещена модель, получает доступ к коду, может его изменять и повторно размешать под своим авторством. Это не является проблемой, если разработчики не намерены получать коммерческую выгоду от разработок. Но, в противном случае или, если эта модель является разработкой предприятия, любой несанкционированный доступ к коду и его дальнейшее использование будет являться нарушением прав на интеллектуальную собственность.

Еще сложнее вопрос обстоит с моделями, созданными при помощи 3D-сканера. Если сканируется творческая работа (фигурка, конкретный дизайн, орнамент, ваза и т.п.), которая не является общественным достоянием, то такие объекты защищены авторским правом с момента создания и за их копирование и распространение можно привлечь к ответственности, если удастся установить виновника. В случае если сканируются полезные образцы, предметы несущие технические и функциональные характеристики, то нужно учитывать, существует ли на них зарегистрированный патент или нет, чтобы их воспроизводить. К тому же, являясь копией с чего либо, модель, полученная сканированием, не может считаться защищенной авторским правом, это означает, что кто угодно может, не спрашивая разрешений, изменять, воспроизводить и использовать такой файл [1, с.16].

В мировой практике еще не достаточно случаев описывающих нарушения прав интеллектуальной собственности предприятий связанных с производством на основе 3D-печати. Компании, которые начали строить свою деятельность, предоставляя независимым разработчикам услуги по сопровождению и дальнейшей реализации их моделей, уже сталкиваются с рядом проблем и вырабатывают пути их возможных

решений. Таких организаций пока немного, и только некоторые из них предоставляют услуги по защите информации своих клиентов. Например, нью-йоркская компания *Shapeways* утверждает, что они проверяют получаемые от разработчиков файлы на сайте на оригинальность, чтобы модель не была просто копией или адаптацией другой модели без разрешения на то ее автора [2]. В *Shapeways* сканируют код и сравнивают с уже имеющимися у них в обработке файлами. Данный способ применим для крупных файлообменных систем, как *Shapeways*, но может оказаться неэффективным на меньших площадках. Поэтому для защиты файлов от несанкционированного доступа сегодня могут применятся распространенные методы защиты цифровой информации: шифрование, перемещение файлов на изолированные сервера с ограниченным доступом или создание файлов, которые не будут функционировать без дополнительной информации.

Но многие специалисты сходятся во мнении, что технологии аддитивного производства настигнет участь современных мультимедиа. И что способы защиты могут применяться те же – DRM (*Digital rights management – Технические средства защиты авторских прав* – программные/программно-аппаратные средства, ограничивающие или затрудняющие просмотр, изменение, копирование файлов мультимедиа, находящихся в электронном доступе); но эффект они будут иметь примерно тот же – будут охватывать незначительную часть ресурсов и будет множество средств обойти ограничения по использованию файлов, например, пользовательские форумы и открытые файлообменики.

В заключении можно сказать, что существующий уровень технологии аддитивного производства и ее потенциал требуют создания новых средств защиты цифровой информации, так как существующие не удовлетворяют нужд лиц, намеренных получать коммерческую выгоду от своих разработок. В целом 3D-печать попадает под существующие рамки защиты интеллектуальной собственности, но с переходом в электронную плоскость, появляется множество проблем, до сих пор не решенных для всех видов цифровых данных. Требуется создание дополнительных программных средств, которые регулировали бы права доступа пользователей к электронным файлам и дополнительных методов борьбы с кибер-пиратством.

Список использованных источников:

1 Weinberg M. It will be awesome if they don’t screw it up: 3D Printing, Intellectual Property, and the Fight Over the Next Great Disruptive Technology // Public Knowledge. – 2010 – nov.10.
2. Baker P. 3D Printers: IT's Next Great Data Challenge // InformationWeek – 2015 – aug.27.

УДК. 621.391

Матвеев Владимир Васильевич
к.ф.-м.н., доцент
Титаренко Виктор Николаевич
ст. преподаватель
Титаренко Дмитрий Викторович
к.э.н., доцент
Институт экономики и управления
ФГАОУ ВО «Крымский федеральный университет им. В.И. Вернадского»
Республика Крым, Россия

ИМИТАЦИОННАЯ МОДЕЛЬ АДАПТИВНОГО КОНТРОЛЯ ДОСТОВЕРНОСТИ ДАННЫХ

Современное развитие информационного сообщества осуществляется на основе сбора, обработки, накопления и обобщения информации. Важное место в этом процессе занимает вопрос оценки достоверности собираемой и накапливаемой информации [2,3].

В работе предложен подход к построению адаптивного контроля достоверности информации на основе имитационного моделирования в среде Powersim [1] , и при котором объем выборки определяется исходя из объема поступающей информации, оценок недостоверности информации (ошибок), полученных на предыдущих этапах (шагах, тактах) контроля.

На рис. 1 представлена потоковая диаграмма, в среде Powersim, имитационной модели решения задачи адаптивного контроля достоверности информации на основе формирования выборки, объем которой зависит от уровня достоверности данных и объема поступающей информации.

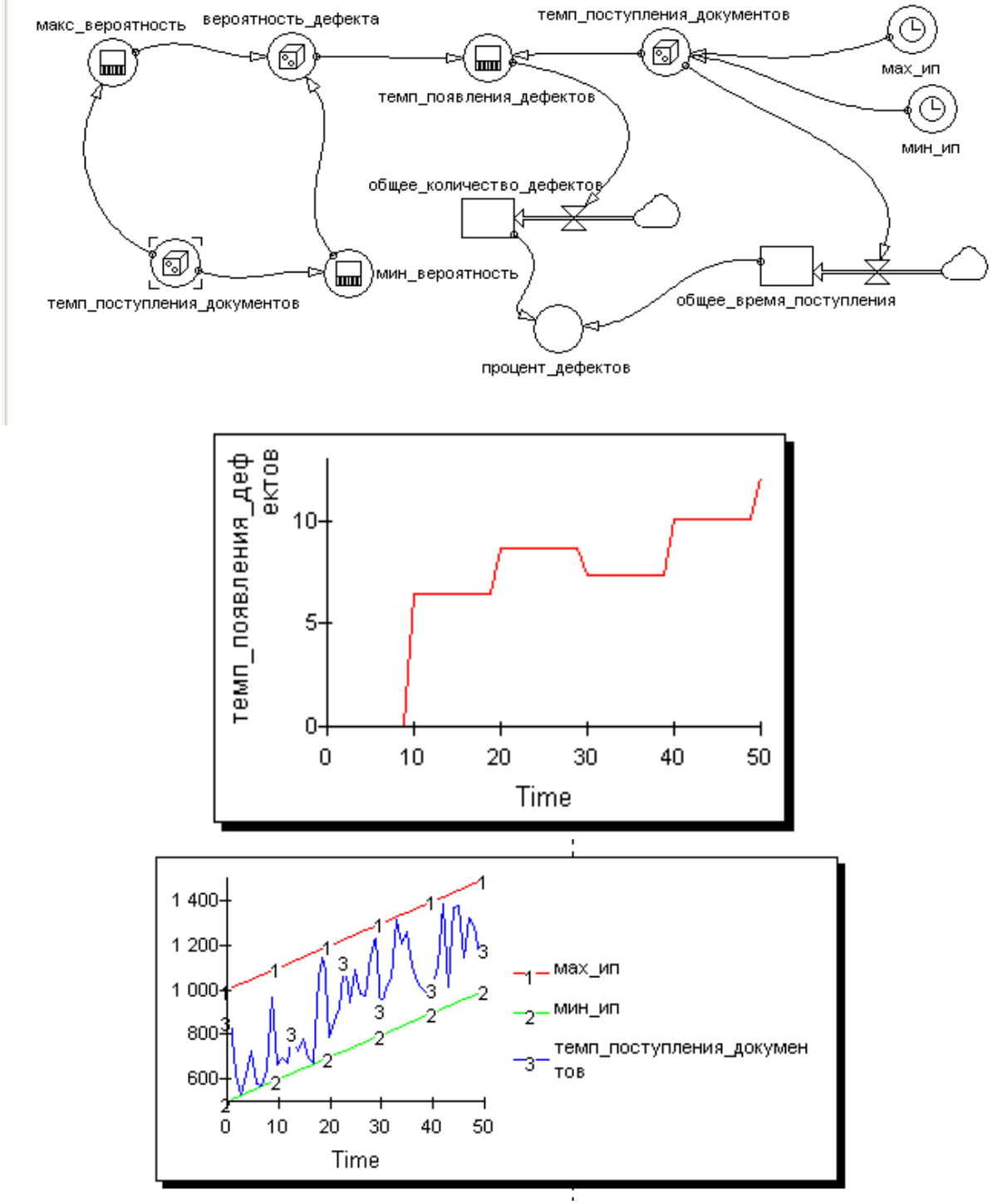


Рис.1. Потоковая диаграмма имитационной модели адаптивного контроля достоверности информации и графики поведения переменных в процессе имитационного эксперимента.

Описание переменных модели.
Уровневые переменные имитационной модели

init общее_количество_дефектов = 0
flow общее_количество_дефектов = +dt*темп_появления_дефектных_данных
doc общее_количество_дефектов = количество дефектных документов, обнаруженных в процессе контроля
unit общее_количество_дефектов = шт.
init общее_время_контроля =0
flow общее_время_контроля= +dt*Темп_поступления_документов
unit общее_время_контроля = номера временных тактов.
Уравнения темпов
aux max_вероятность = 1% * темп_поступления_документов / INIT (темп_поступления_документов)
doc max_вероятность = 1% - верхняя удельная допустимая граница количества дефектных документов.
unit max_вероятность = безразмерная.
aux min_вероятность = 0,5% * темп_поступления_документов / INIT (темп_поступления_документов)
doc min_вероятность = 0,5% - верхняя удельная допустимая граница количества дефектных документов.
unit min_вероятность = безразмерная.
aux темп_поступления_документов = ROUND (RANDOM (min_ип, max_ип))
doc темп_поступления_документов = целая часть случайной величины равномерно распределенной в интервале (min_ип, max_ип).
unit темп_поступления_документов = шт./ед.времени
aux вероятность_дефекта = RANDOM (min_вероятность, max_вероятность)
doc вероятность_дефекта = случайная величина равномерно распределенная в интервале (min_вероятность, max_вероятность)
unit вероятность_дефекта = безразмерная случайная величина
aux количество_дефектов = SAMPLE (темп_производства*вероятность_дефекта, 5, 5)
doc количество_дефектов = выборка с шагом 5 из Темпа_производства на шаге умноженная на вероятность_дефекта
unit количество_дефектов = штук
aux процент_дефектов = (общее_количество_дефектов/ общее_время_контроля)*100%
doc процент_дефектов = общее_количество_дефектов деленное на общее_время_контроля (количество тактов контроля), умноженное на 100%
unit процент_дефектов= процент
aux max_ип = 1000 + (10*TIME)
doc max_ип = максимум поступления документов на такте, TIME - номер временного такта.
unit max_ип = штук
aux min_ип = 500 + (10*TIME)
doc min_ип = минимум поступления документов на такте, TIME - номер временного такта.
unit min_ип = штук

В итоге выполнения работы построена имитационная модель адаптивного контроля достоверности информации, проведен имитационный эксперимент, результаты моделирования представлены на графиках (см. рис.1). Предлагаемый подход к решению задач адаптивного контроля достоверности информации на основе имитационного моделирования достаточно универсален и применим при решении различных задач исследования в экономике.

Литература:

1. Сидоренко В.Н. Системно-динамическое моделирование в среде POWERSIM: Справочник по интерфейсу и функциям. -М.: МАКС-ПРЕСС, 2001
2. Емельянов А.А., Власова Е.А., Дума Р.В. Имитационное моделирование экономических систем, «Финансы и статистика», Москва 2002г.

3. Лысенко Ю.Г., Овечко Г.С., Овечко А.В., В.Н. Кравченко В.Н., Беленко Д.В. Имитационное моделирование экономических систем, Донецк, Юго-Восток 2007г.

Парфенов И. И.
студент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ

Для любой преуспевающей и уважающей себя компании, пользование современными информационно-техническими технологиями стало залогом успешного ведения бизнеса.

Такие технологии упрощают работу предприятия путем автоматизации бизнес процессов и позволяют решать огромный спектр задач, связанных с ведением бизнеса. Помимо большого количества положительных моментов, присутствуют и уязвимости. Большой спектр новых уязвимостей и потенциальных опасностей для информационной деятельности компании был обнаружен, путем автоматизации деятельности предприятия. Пренебрежениями правилами и вопросами информационной безопасности может привести к катастрофическим последствиям для предприятия. [10, 11]

Необходимо учесть, что ни одни технические, организационные и правовые меры не могут гарантировать полную безопасность и надежность современной информационной системы предприятия. Одной из главных и основных задач обеспечения информационной безопасности предприятия, сводиться к снижению рисков.

Понятия «оценка рисков» (Risk Assessment) и «управление рисками» (Risk Management) появились сравнительно недавно и сегодня вызывают постоянный интерес специалистов в области обеспечения непрерывности бизнеса (Business Continuity) и сетевой безопасности (Network Security). Подготовлено более десятка различных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты ISO 17799-2002 (BS 7799), GAO и FISCAM, SCIP, NIST, SAS 78/94 и COBIT.

Разработка и внедрение политики информационной безопасности	2
Мероприятия по работе с персоналом (наведение справок, контроль за поведением, и т.п)	3
Совершенствование организационной структуры	4
Анализ рисков	5
Управление жизненным циклом (управление рисками)	5
Совершенствование должностных инструкций и условий контрактов	5
Меры контроля за посетителями	6
Управление имуществом компании	7
Обучение персонала и контроль за соблюдением режима ИБ	9
Меры контроля за работой приложений	10

Указанные в таблице значения являются ориентировочными оценками эффективности вложений в различные классы мероприятий в области защиты информации. В ряде случаев используются более сложные таблицы, в которых эффективность зависит от ряда факторов.

Список используемых источников:

1. Баранов А.В., Петренко С.А. Системная интеграция и безопасность компьютерных сетей // Конфидент. Защита информации. – 2001. – №2. – С.34–39.

2. Бабин С.А. Аудит сетей как фактор обеспечения безопасности сетей. //М.: Антонюк-Консалтинг. Сети и системы связи №3, 1998.

3. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. //М.: Радио и связь, 2000.

4. Нестеров С.А., Петренко С.А. Программные средства анализа информационных рисков компании // Экспресс-Электроника. – 2002. – №10. – С.84–86.

5. Петренко С.А., Терехова Е.М. Оценка затрат на защиту информации. //. Защита Информации – 2005. – №1.

6. Петренко С.А., Терехова Е.М. Обоснование инвестиций в безопасность. //. Защита Информации – 2005. – №1.

7. Анализ рисков в области защиты информации, Информационно-методическое пособие // ООО «Издательский Дом «Афина», 2009.

8. Kevin J. Soo Hoo. How Much Is Enough? A Risk-Management Approach to Computer Security. Concortium for Research on Information Security and Policy (CRISP), School of Engineering, Stanford University, June 2000. Working Paper.

9. Standards for Information Systems Auditing. — ISACA Standards, 2000.

10. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.

11. Корольов О.Л., Круліковський А.П. Інтелектуальні методи моделювання процесів управляння проектами / Корольов О.Л., Круліковський А.П. // Ученые записки Крымского федерального университета имени В.И. Вернадского. - Экономика и управление. - 2013. - Т. 1. № 26 (65). - С. 73-86.

УДК 659.4

Пенькова Инесса Вячеславовна
д.э.н., профессор
Бурлык Никита Богданович
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ ЗАЩИТА В ТУРБИЗНЕСЕ

Современный уровень развития туристического бизнеса и серьезная конкуренция в этой сфере обуславливают особую важность информационных систем туристских агентств и их защиты. Функциональные возможности этих систем призваны обеспечивать:

- ввод, хранение, редактирование и защиту информации о гостиницах, турах, о состоянии заявок, о клиентах;
- вывод информации в виде необходимых документов: ваучеров, анкет, списков туристов, гостиниц, описаний туров;
- калькуляцию стоимости туров с учетом скидок и курса валют;
- контроль оплаты туров и формирование финансовой отчетности;
- перевод и экспорт-импорт данных в другие программные продукты (Excel, Word, бухгалтерские программы);
- сохранность и защиту персональных данных клиентов и прочие возможности.

Такие системы ускоряют формирование документов и процесс расчетов, дают возможность снижать стоимость услуг (турпакета), путем выбора оптимального ценового варианта доставки клиентов, размещения и т.п. Соответствующая деятельность связана с коммерческими и информационными рисками утечки информации и ее потери в связи со взломами баз данных и ИС

Заказ на создание уникальной информационной системы (ИС) автоматизации офиса туристической направленности стоит достаточно дорого. Однако в настоящее время в этом нет особой необходимости, так как на рынке представлены разнообразные хорошо зарекомендовавшие себя программные продукты (ПП). Разработку специализированных ПП для туристского офиса в настоящее время обеспечивают несколько российских фирм: "Мегатек" (ПП "Мастер-тур"), "Арим-Софт" (ПП "Чартер", TurWin, "Овир"), "Туристские технологии" (ПП комплексной автоматизации "Туристский офис"), "Само-Софт" (ПП "Само-тур"), "Интур-Софт" (ПП "Интур-Софт"), "Рек-Софт" (комплексный ПП "Эдельвейс", "Барсум", "Реконлайн"), ANT-Group (сисистема ANT-Group) и др.

С расширением ИТ и сети Интернет применительно к поиску и бронированию туруслуг, становиться очевидным то, что каждый крупный оператор, работающий на нескольких направлениях, создает собственную систему бронирования и поиска на личном сайте, который целесообразно снабдить защитой от фальсификации и обеспечить безопасный клиентский доступ к ней. Таким образом, крупные многопрофильные туроператоры на современном этапе будут конкурентами поисковых систем или пересекутся интересы туроператоров, так как предлагаемые операторами и поисковиками услуги во многом похожи. В этой ситуации конкуренция между поисковыми системами вырастет в разы, а передовые технологии с обеспеченным безопасным доступом – менее затратные и масштабируемые наиболее перспективны и, разумеется, наиболее креативные, предлагающие множество сервисов системы будут востребованы как туристами, так и турагентствами.

УДК 004.58

Пенькова Инесса Вячеславовна
д.э.н., профессор
Семышев В. В.
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ЗАЩИТА В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Система электронного документооборота (СЭД) связана с совершением сделок и иными действиями и позволяет перейти на безбумажные технологии и автоматизировать процессы использования традиционного бумажного документооборота, что в свою очередь, снижает риски работы электронных систем, применяемых при информационном взаимодействие участников, обеспечивает защиту их прав.

Регламентирующим нормативным документом, при использовании электронных документов в СЭД, являются Правила электронного документооборота. В соответствии с Заключением (№ 14202–03-2115.4 от 15.02.02 г.), на эти Правила Института государства и права РАН, Правила созданы в точном соответствии с положениями законодательства РФ и могут применяться для регулирования и контроля электронного документооборота, в том числе на фондовом, валютном и срочном рынках.

Субъектами взаимоотношений, возникающих в процессе электронного документооборота (ЭД), основываясь на Правилах считают:

- организатора СЭД;
- организатора подсистемы СЭД, в качестве которого выступает юридическое лицо, заключившее с Организатором СЭД договор о выполнении функций Организатора подсистемы СЭД;
- участника СЭД, т.е. юридическое лицо, заключившее с Организатором СЭД договор на участие в СЭД.

Правила вступают в силу в отношении сторон при заключении соответствующего договора между Участником и Организатором об участии в СЭД. После заключения такого Договора Участник СЭД может в установленном порядке получить необходимые средства криптографической защиты информации для использования в СЭД.

Правила ЭД очерчивают общие принципы проведения электронного документооборота между Участниками СЭД и Организатором СЭД, Организаторами подсистем СЭД. Форматы и перечень передаваемых ЭД, порядок их учета, регламент взаимодействия, порядок формирования подтверждений о получении ЭД, правила хранения ЭД и иные особенности документооборота, которые связаны с предоставлением услуг Участникам СЭД, а также характерные черты организации технического доступа к системе электронного документооборота определяются

Биржевыми правилами, нормами Организаторов подсистем СЭД, договорами, заключаемыми между участниками ЭД, в том числе, Организатором СЭД и Организаторами подсистем СЭД.

УДК

Пенькова Инесса Вячеславна
д.э.н., профессор
Серафимова Анастасия Александровна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЗАЩИТА ИНФОРМАЦИИ В РЕКРЕАЦИОННОЙ СФЕРЕ УСЛУГ

Введение. Вопрос о защиты информации весьма актуален. Очень важно предотвратить утечку информации или же несанкционированного, непреднамеренного воздействия на информацию, дабы избежать ущерба. Рассмотрим основные пути защиты информации в рекреационной сфере услуг.

Цель. Выявить меры по защите информации в рекреационной сфере услуг.

Результаты исследования. Рекреационная сфера услуг является весьма обширным понятием. Важное место среди отраслей социальной сферы принадлежит активному отдыху населения, иначе говоря, рекреации.

Рекреация понимается как активный отдых населения, средство восстановления физических и духовных сил.

Как элемент социальной сферы, рекреация способствует удовлетворению культурных потребностей населения.

Потребность в рекреационных услугах является комплексной и включает в себя совокупность частных потребностей, представляющих — физическую, духовную, интеллектуальную, эмоциональную, социальную потребности.

Туризм - одна из важнейших сфер в рекреационной сфере услуг, по удовлетворению потребностей человечества.

Совокупность всей информации, необходимой для функционирования туристской системы на том или ином уровне управления, представляет собой информационную базу данных туризма, которая нуждается в защите.

Иначе говоря, информационная база данных туризма и специализированные информационные технологии, предназначенные для ее обработки, которые обеспечивают эффективное функционирование туристской системы на различных уровнях управления туризмом могут быть подвержены взлому, утечке информации. Туристические агентства имеют в своей базе данных огромное количество анкет с персональными данными их клиентов. Все туристические компании, использующие в своей деятельности персональные данные туристов, должны осуществить мероприятия по их защите.

Обеспечить сохранность персональных данных, находящихся в базе данных туристской организации позволят электронные программы.

Но полностью исключить вероятность кражи базы данных нельзя. Можно лишь, помешать это сделать, например, расписать права доступа, парольная защита, шифрование данных и программ, установление прав доступа к объектам БД.

Кроме внутренних информационных угроз, есть угрозы внешние. Это хакеры, которые могут взломать сайт, проникнуть в локальную систему, обмануть пользователей. Причем эксперты не исключают, что в роли хакеров могут выступить разработчики софта: руководителям туристических компаний, надо понимать, что именно делает купленная ими программа, не отправляет ли она конфиденциальную информацию конкурентам? Софт, с помощью которого обрабатываются персональные данные клиентов, должен быть сертифицирован. Защититься от внешних угроз полностью нельзя, можно лишь снизить тяжесть последствий. Разработать лишь, например, шаблоны действий сотрудников в случае ЧП.

Согласно инструкции, разрешенными к сохранению являются имя, фамилия, пол, дата рождения, адрес проживания, электронный адрес, номера телефонов, средство оплаты путешествия , даже (бронирование отеля или аренда автомобиля), туристические предпочтения, конечная или промежуточная цели путешествия, даты путешествия, данные паспорта или иного удостоверения личности, подробности визы, сведения о партнерах по заключению туристического договора или родственниках основного туриста, если тур приобретается не для одного человека. Каждому договору соответствует его собственный номер, что позволяет сотруднику быстро сориентироваться в громадной базе данных и способствует оперативной работе при обслуживании клиентов.

Туристические компании, которые владеют сведениями о клиентах в более широком диапазоне — от номерных знаков автомобиля, постоянного адреса, места проживания в отпуске до имен напарников по путешествию, в первую очередь обязаны соблюдать закон о неразглашении конфиденциальности информации, нарушение которого предусматривает административную, уголовную и дисциплинарную ответственность и карается по статьям. За нарушение установленного порядка сбора, хранения и использования персональных данных граждан установлена административная ответственность в ст. 13.11 КоАП РФ. Штраф для должностных лиц составляет от 500 до 1000 рублей, для юридических лиц - от 5000 до 10 000 рублей.

Защита конфиденциальных данных предусмотрена ст. 13.14 КоАП РФ. Если лицо, получившее доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, разгласило ее, то на него будет наложен административный штраф в размере от 4000 до 5000 рублей.

Вывод: Таким образом, в результате проведенных исследований были выявлены основные пути по защите информации в рекреационной сфере услуг. Из всего вышесказанного можно сделать вывод, что защита информации в рекреационной сфере услуг играют большую роль, хоть мы и более детально изучали сферу туризма, но тем не менее любая и другая отрасль в рекреационной сфере направлена на работу с персональными данными клиентов, например, оздоровительные комплексы, санатории и т.п. и поэтому тоже нуждается в защите информации и в комплексе различных мер.

К сожалению, не существует программного обеспечения позволяющего полностью защитить базы данных клиентов, но тем не менее, существует перечень мер, которые помогают уменьшить риск кражи персональной информации пользователя. А также, в защите информации помогают административные и уголовные наказания, действующее в наше время.

УДК 659.4

Пенькова Инесса Вячеславовна
д.э.н., профессор
Халлиев Бахром Бахтиерович
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ ЗАЩИТА В РЕКЛАМНО-КОММУНИКАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

В современных условиях реклама стала одним из факторов конкурентного соперничества, не менее важным, чем достижение преимущества в сегменте рынка внедрением технических инноваций или снижения издержек и себестоимости продукции. Сегодня реклама является практически единственным действенным инструментом влияния на рынок. Она все в большей мере выполняет функцию управления потребительским спросом, который представляется составляющей системы маркетинга. В настоящее время конкуренция за привлечение потребителя приобретает все более утонченные оттенки, что приводит к определенным сложностям. Совершенство и новизна товара или услуги для покупателя теперь часто важнее цены.

Таким образом, на современном рынке одерживает победу тот, кто предлагает принципиально новые товары или более безупречный сервис, методы и формы сбыта и пост продажных услуг.

Достижение коммерческого успеха и повышение эффективности рекламной деятельности требует от компании выстраивать отношения со всеми заинтересованными сторонами на основах открытости, честности и взаимовыгодного сотрудничества. Передавая коммуникационные обращения различным целевым аудиториям, следует позаботиться о том, чтобы в общем информационном потоке не присутствовала информация, составляющая коммерческую тайну. которая делится на группы: научно-техническая информация; производственная информация, финансовая информация.

Анализ показал, что рекламные расходы и затраты на проведение акций и промо-мероприятий увеличились, но при этом процент эффективности коммуникационной деятельности незначительно, но тоже вырос.

В современных условиях напряженной конкурентной борьбы для получения дохода, магазинам спортивного инвентаря придется использовать разные способы завоевания клиента. Магазин не будет исключением в борьбе за лидерство на рынке спортивных товаров и услуг, поэтому потребуется не только применять успешные и зарекомендовавшие себя методы конкуренции, но и формировать новые способы привлечения клиентов. Среди таких инноваций есть активное введение деятельности магазина в интернет-режим с помощью форумов в интернет-журналах, в которых потребители имеют возможность разместить свои отзывы, а, следовательно, позитивную или негативную рекламу относительно товара магазина. Для магазина это является эффективным инструментом привлечения потребителей приобрести товары или воспользоваться услугами предприятия.

Эффективность рекламы представляется экономическим результатом, который получен в результате применения рекламного инструмента или проведения кампании. Эффективность психологического влияния рекламы на покупателя определяется с помощью опросов, экспериментов и наблюдений. Обеспечение информационной безопасности представляется одним из направлений рекламно-коммуникационной деятельности. Защита коммерческой тайны предотвращает кризисные ситуации и усиливает безопасность предприятия в целом.

УДК 685

Попов Виталий Борисович
к.ф.-м.н., доцент
Кузькина Екатерина Андреевна
магистрант
Институт экономики и управления
ФГАОУ ВО «Крымского федерального университета им. В.И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СУБД ORACLE

Цель работы анализ организации и реализации вопросов обеспечения защиты персональных данных в системах управления базами данных, в частности СУБД ORACLE.

Классическая схема защиты баз данных (БД) подразделяется на следующие обязательные процедуры:

1. **Разграничение доступа.**

Преследуя цель защиты БД от инсайдерских угроз, для обеспечения разграничения доступа в версии СУБД 10g Release 3 компания Oracle выпустила продукт Database Vault, предназначенный для предотвращения несанкционированного доступа к информации пользователей, в том числе наделенных особыми полномочиями, например, администраторов базы данных. Набор правил в Database Vault, разграничивающих доступ, достаточно широк.

2. **Защита доступа.**

Oracle предоставляет разнообразные способы аутентификации и позволяет применять один или несколько из них одновременно. Общим для всех этих способов

является то, что качестве субъекта аутентификации используется имя пользователя. Для подтверждения его подлинности может запрашиваться некоторая дополнительная информация, например, пароль. Аутентификация администраторов СУБД Oracle требует специальной процедуры, что обусловлено спецификой должностных обязанностей и степенью ответственности этого сотрудника. Программное обеспечение Oracle также зашифровывает пароли пользователей для безопасной передачи по сети.

Способы аутентификации в СУБД Oracle:

* ***Аутентификация средствами операционной системы.*** Ряд операционных систем позволяют СУБД Oracle использовать информацию о пользователях, которыми управляет собственно ОС. В этом случае пользователь компьютера имеет доступ к ресурсам БД без дополнительного указания имени и пароля – используются его сетевые учетные данные. Данный вид аутентификации считается небезопасным и используется, в основном, для аутентификации администратора СУБД.

* ***Аутентификация при помощи сетевых сервисов.*** Данный вид аутентификации обеспечивает опция сервера Oracle Advanced Security. Она предоставляет следующие службы:

- SSL - аутентификация использует протокол SSL (Secure Socket Layer) – протокол уровня приложений. Он может использоваться для аутентификации в БД и в общем случае (если далее используется аутентификация пользователя средствами СУБД) не зависит от системы глобального управления пользователями, обеспечиваемой службой каталога Oracle - Oracle Internet Directory.
- Аутентификация службами третьих сторон.

На основе Kerberos. Применение Kerberos как системы аутентификации с доверенной третьей стороной, основано на использовании общего секрета. Это предопределяет безопасность и надежность доверенной стороны и дает возможность использования Single Sign – On, централизованного хранения паролей, прозрачной аутентификации через связи БД (database links), а также средств усиленной безопасности на рабочих станциях.

На основе PKI. Применение PKI для аутентификации предполагает издание цифровых сертификатов для пользователей (приложений), которые используются для непосредственной аутентификации на серверах БД в рамках одной организации. При этом не требуется использование дополнительного сервера аутентификации. Oracle определяет следующие компоненты для использования PKI:

- протокол SSL,
- набор OCI (Oracle Call Interface – прикладной интерфейс доступа к БД) и PL / SQL функций,
- доверенные сертификаты (trusted certificate), для проверки подлинности сертификатов, предъявляемых пользователями (приложениями),
- Oracle wallets – ключевые контейнеры, содержащие личный ключ (private key) пользователя, его сертификат и цепочки доверенных сертификатов,
- Oracle AS Certificate Authority – компонента Oracle Application Server, предназначенная для издания сертификатов и дальнейшего управления ими,
- Oracle Wallet Manager (OWM) - компонента СУБД для управления валлетамми.

На основе RADIUS. СУБД Oracle поддерживает протокол RADIUS (Remote Authentication Dial – In User Service) – стандартный протокол для аутентификации удаленных пользователей. При этом становятся доступны службы и устройства аутентификации третьих производителей, с которыми может взаимодействовать сервер RADIUS (например, устройства генерации одноразовых паролей, биометрические устройства и т.п.).

На основе службы LDAP – каталога. Использование службы LDAP -каталога делает управление аутентификацией и управление учетными записями пользователей (приложений) очень эффективным.

В инфраструктуре СУБД Oracle служба каталога представлена следующими компонентами:

- Oracle Internet Directory (OID) позволяет централизованно хранить и управлять информацией о пользователях. Позволяет иметь единственную учетную запись пользователя для многих баз данных. Возможна интеграция со службами каталогов третьих производителей. OID позволяет гибко управлять атрибутами безопасности и привилегиями каждого пользователя, включая тех, кто аутентифицируется по цифровым сертификатам. Для повышения безопасности во время процесса аутентификации возможно использование SSL -протокола.
- Oracle Enterprise Security Manager - утилита управления пользователями, группами, ролями и привилегиями.

**** Аутентификация в многоуровневых приложениях.***

Приведенные выше методы аутентификации также могут быть применены и в многоуровневых приложениях. Как правило, для доступа к приложениям из сети Интернет используется аутентификация по имени и паролю (в том числе с использованием протокола RADIUS), либо по протоколу SSL. Прочие методы используются для работы пользователей в локальной сети.

3. Шифрование данных

Для защиты данных, передаваемых в сети, в СУБД Oracle, начиная с версии 8i, используется возможности опции Oracle Advanced Security, в которой предусмотрена функция Network encryption, позволяющая шифровать весь поток данных. Безопасность информации обеспечивается секретностью ключа, которым шифруются данные.

Network encryption позволяет добиться высокого уровня безопасности. Поддерживаются следующие алгоритмы шифрования AES (только 10 g /11g). DES, 3 DES, RC 4 (только 10 g /11g).

Защита передаваемых в сети данных в приложениях Oracle обеспечивается протоколом SSL по алгоритмам, которые поддерживается сервером приложений, как правило, это WEB – сервер Oracle.

Защиту данных на носителе обеспечивают два компонента СУБД Oracle – пакеты, реализующие алгоритмы шифрования и опция Transparen t Data Encryption (TDE). Начиная с версии 8i, СУБД Oracle предоставляет для разработчиков приложений пакеты хранимых процедур, реализующих алгоритмы: DES с длиной ключа 56 бит, Triple DES с длиной ключа 112 и 168 бит, AES с длиной ключа 128, 192 и 256 бит RC 4 (только 10 g /11g). Опция T DE появилась в версии СУБД Oracle 10g Release 2 как составная часть Advanced Security. Она позволяет выборочно шифровать колонки таблиц с применением алгоритмов Triple DES (с длиной ключа 168 бит), AES (с длиной ключа 128, 192 или 256 бит). Управление ключами шифрования берет на себя ядро БД, а применение такого шифрования не требует переделки клиентского и серверного прикладного ПО. В версии СУБД 11g и выше появилась возможность шифрования табличного пространства целиком.

4. Аудит доступа к данным

СУБД Oracle имеет мощные средства аудита действий пользователей, включающих как доступ к данным, так и события регистрации/выхода и изменения структуры БД. Начиная с версии 9i, СУБД оснащается опцией подробного аудита (Fine Grained Audit Control), которая позволяет проводить аудит доступа по условиям, определяемым достаточно гибкими настраиваемыми правилами. Однако, данные средства аудита не позволяет проследить за действиями, которые совершаются администратором базы данных, а также не мешают ему изменять журнал аудита, удаляя любые строки и не оставляя следов подобных действий.

Возникшая необходимость аудита деятельности и защиты данных аудита от привилегированных пользователей, включая администраторов БД, побудило Oracle разработать новую концепцию аудита. В её основу положена идея, на которой базируется функционал Database Vault: администратор БД изолирован от управления аудитом. Как и в случае Database Vault правила назначения аудита в Audit Vault очень гибкие.

В настоящее время требования к безопасности со стороны потребителей достаточно высоки, и оптимальное решение состоит в полноценном использовании встроенных средств безопасности и разумным их дополнением продуктами и решениями сторонних разработчиков, таких как Oracle.

УДК 378.14: 004. 056. 5

Семёнова Л. С.
старший преподаватель
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

О НЕКОТОРЫХ ПРОБЛЕМАХ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

В настоящее время, время экономических кризисов и жёсткой политической борьбы, особое развитие получило уродливое явление - манипулирование людьми посредством использования различных средств и технологий информационно-психологического воздействия. Понимание угроз информационно-психологической безопасности (ИПБ) личности, механизмов их действия и возможностей психологической защиты становится не только научной проблемой в рамках теории информационной безопасности, но и насущной необходимостью в повседневной жизни человека.

Человек представляет собой открытую информационную систему. Информацию человек получает через сенсорные каналы – «входы» из непосредственного опыта, общения, из источников информации (книги, Интернет, СМИ и т.п.). Замечено увеличение доли информации, получаемой из информационных источников, нежели из непосредственного опыта и личного общения. Информация в процессе усвоения проходит следующие фильтры: нейрофизиологический, социальный, индивидуальный. Механизмы манипулирования учитывают природу усвоения человеком информации. Информация в информационном обществе становится стратегическим ресурсом. Идет невидимая торговля знаниями, культурой. В информационном поле, переплетаясь, одновременно сосуществуют истинная и ложная информации, что с успехом может вводить в заблуждение окружающий мир, нанося ущерб человеческим ценностям. Искажение нравственных норм, социальных установок влияют на процессы общественной, политической и экономической жизни общества. Влиянию информации подвержена духовная сфера общества, что приводит к социальной напряженности. Под влиянием информационной среды происходит изменение психических состояний людей. Это обусловлено субъективностью человека и сложностью познания истины о мире. Назрела необходимость проводить активную работу по информационной и психологической безопасности личности, чтобы защитить психику человека от неблагоприятных информационных факторов. Для современного человека «сетевой компьютер» превратился в главный источник информации.

Формирование информационной культуры является первостепенной задачей высших учебных заведений. Важно научить интерпретировать информацию, понимать ее суть, принимать личностную позицию по отношению к скрытому смыслу, находить требуемую информацию в различных источниках, систематизировать ее, находить ошибки в получаемой информации, воспринимать альтернативные точки зрения и высказывать обоснованные аргументы, устанавливать связи, вычленять главное в информационном сообщении. Разработка и реализация комплекса мероприятий предотвращения и нейтрализации негативных информационно-психологических воздействий должна стать важной частью работы ВУЗа. Целесообразно организовать проведение исследований, направленных на изучение проблем информационно-психологической безопасности личности, создания эффективной системы ее психологической защиты, разработку и внедрение современных педагогических технологий формирования психологической самозащиты человека в процессе обучения в системе образования.

Литература:

1. Грачёв Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты/ [Электронный ресурс] / Г.В. Грачёв //. – Режим доступа: http://www.rus-lib.ru/book/32/Yrid_psihologiaj/Gracev/Gratev.htm

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
Шелуха Ольга Сергеевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДИСТАНЦИОННОМ ОБРАЗОВАНИИ

В настоящее время в связи с быстрыми темпами развития новых информационных технологий, появляются и новые подходы к организации образования. Одним из них является дистанционное образование, которое понимается как открытая система обучения, предусматривающая активное общение студента с преподавателем с помощью современных технологий и мультимедиа. Такая форма обучения позволяет свободно выбрать время и место учебы, что бывает полезным для инклюзивного образования, работающих или иностранных студентов, а так же студентов, которые учатся по программе обмена опыта некоторое время в вузе другого государства.

Обоснование необходимости применения технологий дистанционного и смешанного обучения, психолого-педагогические особенности, возможности и преимущества такой формы обучения рассматриваются в последних научных исследованиях Анисимова А.М., Гороховского О.И., Джонсона Б., Капустина Ю.И., Курмышева Н. В., Кухаренко В.Н., Рашевского Н.В. и др.

Информационную безопасность в системах дистанционного образования необходимо рассматривать с опорой на законодательные акты. В доктрине информационной безопасности Российской Федерации, утвержденной Президентом выделены основные интересы личности, общества и государства [2]. К проблемам информационной безопасности в системе дистанционного образования можно отнести защиту от разнообразных видов мошенничества и защиты информации, которая не соответствует нормам морали, а также такому дидактическому принципу как научность.

Передача данных в дистанционной среде обучение требует защиты информации. Информационная безопасность выделяет три основные аспекта:

- целостность – предназначена для проверки достоверности и полноты информации, а также для методов обработки;
- доступность – обеспечения доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости;
- конфиденциальность – позволяет получать доступ к информации только авторизованным пользователям.

Практически все информационные системы защищены с помощью аутентификации пользователя. Ведущие компании в области сетевых технологий, в частности в сфере удаленного обучения, реализуют, помимо технологии организации доступа по логину и паролю, обязательную иерархию пользователей с поддержкой многоуровневой системы распределения ролей и различные методы шифрования передаваемых данных. Благодаря криптографическому преобразованию данных поддерживается функция конфиденциальности при передаче информации. На сегодня используют комбинации симметричного и ассиметричного методов шифрования для максимальной степени защиты информации. Системы шифрования протокола, система паролей не дают нам 100% гарантии в основном вся информация сохраняется в кэше браузера, чем создает возможность утечки информации. Чтобы избежать подобных ситуаций используют передачу паролей, зашифрованных открытым ключом, созданных на время сеанса.

Проблемы информационной безопасности возрастают с каждым днем, особое внимание стало уделяться проблемам борьбы и сотрудничества в образовательной деятельности. Уделяется внимание и вопросам связанных с несанкционированным

доступом к персональным данным студентов и к учебным материалам, проблемы обеспечения надежности функционирования информационных систем учебного назначения [1].

Информационные угрозы в дистанционной среде обучение не особо отличается от угроз в любой информационной системе. В первую очередь угрозы связаны со случайными факторами, ошибками персонала и тьютора, а также влиянием внешних факторов, к которым можно отнести несанкционированный доступ. Все эти проблемы находят решения в дистанционной среде обучения. Можно выделить еще одну проблему – это размещение «псевдоучебных» материалов пользователями, не имеющими должной квалификации и компетенции и наносящими вред всем, кто с этими материалами знакомится и принимает на веру изложенные в них сведения. Даже человек с высоким уровнем подготовки не всегда может заметить искажение тех или иных фактов или проблем что приводит к подмене истинных знаний. Ни одно техническое средство не способно бороться с подобной угрозой. Решение данной проблемы требует отдельного рассмотрения, целесообразно создавать группы, коллективы, экспертные комиссии проверяющие и фильтрующие информацию.

Использование технологий дистанционного обучения предоставляет студенту огромный простор для самостоятельной деятельности, формирует у него способности к самообразованию, самосовершенствованию, самопознанию, само информированию, формирует умение получать необходимую информацию и ее обрабатывать. Важную роль в системе дистанционного образования играют как участники процесса обучения, так и бизнес-процессы, регламенты, средства защиты информации, курсы, цели. Дистанционное образование в обществе, испытывающем нарастающую потребность в знаниях, должно быть совершенным и безопасным. Угрозы информационной безопасности существуют и они нуждаются в тщательном исследовании с целью поиска эффективных путей их предупреждения и устранения.

Список литературы:

1. Информационная безопасность в системах открытого образования Колгатин А. Г. – Режим доступу :http://ifets.ieee.org/russian/depository/v17_i1/pdf/6.pdf
2. Доктрина информационной безопасности Российской Федерации от 09.09.2000г N ПР-1895. – Режим доступу : http://www.femida.info/14/19002.htm
3. Федорус А. Н. Проблемы защиты информации в условиях массовой непрерывного образования для всех / Н. Федорус // Современное образование и наука в Украине: традиции и инновации: Материалы XII Всеукраинской научно-практической заочной конференции «Современное образование и наука в Украине: традиции и инновации ». - Том 1 (м. Харьков, 30-31 января 2012г.). - Харьков: 2012. - С. 120-123. - Режим доступа: http://novaosvita.com.ua/wp-content/uploads/2011/10/Kharkiv_XII_OSVITANAUKA_PART1.pdf

УДК 004.056.53

Бойченко Олег Валерьевич
д.т.н., профессор
Адарчина Светлана Олеговна
студентка 4 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЗАЩИТА ЛЕНДИНГА ОТ КОПИРОВАНИЯ

Проблемы сетевой информационной безопасности в настоящее время приобретают все большую актуальность, в связи со стремительным ростом сетевых сервисов как коммерческого, так и потребительского характера.

В работах [1,2] проведен анализ проблем защиты маркетинговой информации сайтов, прежде всего, связанных с довольно эффективным и простым способом доступа к коммерческим данным сайта компании с помощью веб-аналитики.

Установлена необходимость проведения дальнейших научных исследований по разработке системы методов и способов эффективного противодействия мониторингу

сайтов конкурентами для защиты коммерческой рекламной информации о своём продвижении сайта и способах эффективного привлечения клиентов с помощью Интернет-технологий.

Целью работы является анализ проблематики сетевой информационной безопасности в части защиты коммерческих данных целевого сайта (сайта-лендинга), что связано с простотой копирования данных целевой веб-страницы.

В таком случае злоумышленник получает возможность реализовать экономию своего бюджета и времени за счет создания копии, с использование примера привлекательного сайта с удачным предоставлением информации.

Практический опыт показывает, что современная проблематика копирования лендинга, прежде всего, связана с потерей уникальности дизайна владельца сайта за счет модификации злоумышленниками большей части текстового наполнения и изменения контактных данных [3].

Особую опасность представляет целенаправленное копирование лендинга для того, чтобы работать от имени владельца сайта.

Исследования показывают, что в такой ситуации злоумышленники меняют только контактная информация, а персональные данные владельца сайта не меняются.

Так, злоумышленники от имени компании могут предоставлять услуги при неопределенном уровне качества, проводить продажу с предоплатой копий продукции под видом оригинала. Такая ситуация приводит к созданию угрозы потери репутации сайта и потере части трафика, обусловленной деятельностью недобросовестных конкурентов по продажам.

Приведенные примеры обуславливают необходимость создания эффективной системы защиты данных сайта-лендинга от копирования в условиях его открытости во всеобщем доступе.

По нашему мнению, в таком случае необходимо использовать «плавающие» (применяемые избирательно с соответствие с ситуацией) методы противодействия копированию данных сайта:

- использование скриптов запрета клика правой кнопкой мышки на сайте для защиты уникального контента (отключается возможность выделения, копирования и вставки);
- добавление водяного знака к изображениям также может создать необходимые условия противодействия копированию данных, однако не гарантирует того, что злоумышленники не получат заинтересовавшей их информации;
- использование скрипт трекинг-системы, которая своевременно уведомит владельца о месте запуска сайта. При этом трекинг-система (если она не была удалена) обеспечивает даже удаление сайта с уникализированным контентом и значительно измененным дизайном;
- обращение к администратору хостинга по нарушению авторских прав, связанных с использованием злоумышленниками дизайн/ кода сайта.

Таким образом, в результате проведения научного исследования определена основная проблематика информационной безопасности сайта-лендинга от копирования, а также предложен комплекс мероприятий на основе избирательной политики безопасности по защите коммерческих данных владельца сайта.

Список литературы

1. Бойченко О.В. ВЕБ-аналитика конкурентов / О.В. Бойченко, С.О. Адарчина // Актуальные проблемы и перспективы развития экономики: XIV Междунар. науч.-технич. конф., 12-14 ноября 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 237.

2. Бойченко О.В. Проблема защиты маркетинговой информации сайтов / О.В. Бойченко, С.О. Адарчина // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 окт. 2015 г.: материалы конференции / СПОИСУ. – СПб., 2015. – С. 203-204.

3. Ash, Tim. Landing Page Optimization: The Definitive Guide to Testing and Tuning for Conversions. – Wiley Publishing, 2011. – 384 p.

УДК 004.056.57

Бойченко Олег Валерьевич
д.т.н., профессор
Кравцов Игорь Олегович
студент 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СЕТЕВАЯ АТАКА «ОТКАЗ В ОБСЛУЖИВАНИИ»

В работе проводится исследование одного из распространенных видов сетевых атак типа «отказ в обслуживании». Это обусловлено не только распространённостью, но и тем, что для своей реализации они требуют минимум знаний и умений, а также отсутствием надежной защиты от данного вида угроз информационной безопасности информационных управляющих систем. Ввиду своей безнаказанности, масштабы DoS-атак растут и механизмы их проведения эволюционируют.

Целью работы является исследование причины и механизмов сетевых атак типа «отказ в обслуживании», а также методов защиты от основных видов Dos-атак.

Наиболее опасным видом атаки является DDoS-атака. Борьба с атаками «отказ в обслуживании» главным образом осуществляется на уровне хостинга-провайдера, но стопроцентных методов защиты на данный момент не существует.

DoS-атака (от англ. Denial of Service – отказ в обслуживании) - это действия хакеров, вызывающие перегрузку того или иного технологического элемента в цепочке, в результате чего легальные пользователи не могут получить доступ к предоставляемым ресурсам. Это происходит из-за того, что любой веб-сервер имеет ограничения на максимальное количество посещений за определённый период времени и так называемые «паразитные» запросы забивают всё пространство, а для обычных пользователей сайт оказывается заблокированным.

Эксперты в области сетевых атак выделяют 2 основные группы причин использования DoS-атак:

1. Dos-атаки, осуществляемые из личных побуждений (личная неприязнь, месть, развлечение, политический протест);
2. Dos-атаки, осуществляемые с коммерческой целью (шантаж, вымогательство, заказ такой атаки недобросовестным конкурентом).

Отдельно выделяю «случайные» или «нечаянные» DoS-атаки. Они возникают, когда веб-сайт посещают неожиданно большое количество легальных пользователей.

Самая простая DoS-атака может быть выполнена с помощью одного компьютера, специальной программы и высокоскоростного интернета. Ввиду своего примитивизма такая атака не будет иметь успех. Так как современный Интернет позволяет отфильтровать хостинг-провайдеру слишком интенсивный поток запросов по IP-адресу злоумышленика.

Опасной разновидностью DoS-атаки является распределённая DoS-атака (DDoS – Distributed Denial of Service). DDoS-атака состоит в том, что запросы на веб-сайт посылаются одновременно со множества компьютеров, с различных IP-адресов. Для реализации этого вида атак злоумышленники использую так называемые ботнеты. Ботнет- сеть компьютеров, зараженных программами-червями, которые позволяют злоумышленнику выполнять некие действия с использованием ресурсов этого компьютера. Крупные ботнеты могут включать в себя десятки и сотни тысяч компьютеров. Эффективным способом осуществления DDoS-атаки является отправка машинами-зомби запросов к веб-серверу, которые потребуют существенных затрат вычислительных ресурсов на обработку. Обязательно запросы передаются по протоколу HTTP, что сильно затрудняет решение задачи автоматической фильтрации «вредоносных» запросов к серверу до их обработки.

К сожалению, универсальных и абсолютно эффективных методов защиты от всех видов DoS-атак не существует. Всё же используются различные защитные инструменты, затрудняющие проведение атак и снижающие ущерб от атак. Защита веб-сайта от DoS-атак начинается на уровне CMS: программный код CMS должен быть хорошо

оптимизирован, публикуемый контентобязательно кешируется, а количество «точек создания нагрузки» должно быть сведено к минимуму.

Таким образом, результаты исследования указывают, ято наиболее эффективным способом обеспечения безопасности являются защитные инструменты провайдера. Он обладает подробной информацией о характеристиках атаки и может в деталях наблюдать направления её развития. Хостинг-провайдер может «зафильтровать» атаку таким образом, что «атакующие запросы» просто не будут доходить до атакуемого сервера, при этом сохранится доступность сервера для запросов добросовестных посетителей. Программно-аппаратные комплексы провайдера могут обнаруживать атаки как просто в автоматическом режиме так и в автоматическом режиме применяющим контрмеры.

УДК 003.26

Бойченко Олег Валерьевич
д.т.н., профессор
Тупота Елена Сергеевна
студентка 3 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МЕНЕДЖЕР ПАРОЛЕЙ В РЕШЕНИИ ПРОБЛЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ

Целью исследования является проведение анализа основных преимуществ и недостатков использования менеджера паролей в решении проблем сетевой информационной безопасности, а также представить конкретные решения для поддержания необходимого уровня конфиденциальности данных информационной системы управления.

Анализ современной практики использования сервисов Интернет указывает на возникновение необходимости применения в базе данных автоматизированной системы специального «контейнера» для хранения паролей, что обусловлено целесообразностью организации системы сетевой безопасности. Основой системы является современный пароль, представляющий собой комбинацию символов различного регистра.

Применение специального программного обеспечения (менеджер паролей) обеспечивает решение задачи хранения паролей в строго определенном месте, для чего используются специальные зашифрованные файлы с личными данными.

Следует отметить, что некоторые компании предлагают решение в виде расширения для браузера, которое автоматически осуществляет заполнение необходимых форм (Dashlane, LastPass, KeePass, 1Password, PasswordBox, Blur, RoboForm, StickyPassword) как на платной так и на безоплатной основе.

Для последующего анализа целесообразно представить классификацию современных менеджеров паролей по назначению:

- десктопное приложение обеспечивает осуществление процесса хранения паролей к программному обеспечению, установленному непосредственно на жесткие накопители компьютера;
- портативное приложение обеспечивает осуществление процесса хранения паролей к программному обеспечению на мобильных устройствах, смартфонах, портативных накопителях;
- сетевые ресурсы обеспечивают осуществление процесса хранения паролей в режиме онлайн, предоставляя доступ к ним по запросу пользователя.

Кроме того, менеджер паролей может быть использован для дополнительной защиты от фишинга за счет того, что менеджер при обращении со скриптами переходит на фишинговый сайт без подставления данных в форму-ввода (при этом пользователь обязательно оповещается о посещении подозрительного сайта).

Однако, несмотря на достоинства, использование менеджера паролей отличатся рядом уязвимостей. Так, если основной пароль будет взломан, то в руках злоумышленника окажется доступ ко всем пользовательским ресурсам. Кроме того, пароль может быть выявлен с помощью акустического крипто анализа. Ситуация

обостряется в случае использования некоторыми менеджерами паролей включения опции генератора паролей для повышение уровня шифра (в такой ситуации алгоритм генерации так же может выступить в роли инструмента для взлома).

Рассмотрим критическую уязвимость на примере LastPass. Данный сервер является весьма популярным среди пользователей благодаря его бесплатной цене и интуитивно понятному интерфейсу. Однако данный сервер испытывал проблемы с кибер-безопасностью. Так, летом 2015 года сервис был взломан и личные данные пользователей попали к злоумышленникам. Пользователи обнаружили, что двухфакторная защита не полностью обеспечивает сохранность личных файлов пользователей. Шон Кессиди, обнаруживший уязвимость, придумал специальный инструмент – «LostPass» для демонстрации «дырки» в защите сервиса.

Данная уязвимость заключается в том, что, при конкретных условиях LastPass уведомляет пользователя о истечении срока сессии и необходимости прохождения повторной аутентификации. Инструмент придуманный разработчиком использует XSS уязвимость для того чтобы обнаружить есть ли у пользователя аккаунт в LastPass, войдя в него с помощью CSRF, а после выдать уведомление, предлагающее пользователю зайти в свой аккаунт еще раз. Когда пользователь соглашается, с точностью до пикселя появляется логин-страничка LastPass, и введенная пользователем информация передается злоумышленнику.

Кроме того злоумышленник может подделать полномочия для LastPass API-интерфейса, проверить их подлинность, и даже задать конкретного пользователя использующего двухфакторную аутентификацию. Если все условия соблюдены, и все коды прошли проверку, используя тот же LastPass API, злоумышленник может собрать все данные из пользовательского аккаунта, в том числе конкретные пароли от конкретных ресурсов. Стоит учесть, что данная уязвимость работает исключительно в браузер Google Chrome, так как другие браузеры используют другой тип вывода уведомлений с данного веб-ресурса.

Анализ указывает, что все пользователи с двух факторной защитой (все бесплатные аккаунты) находятся в группе риска.

Таким образом, современному пользователю необходимо пользоваться менеджерами паролей, однако пользователи одного из сервисов LastPass, использующие браузер от компании Google подвергают опасность своих пользователей. Для того чтобы предотвратить утрату персональных данных и конфиденциальных паролей необходимо использовать ввод данных на странице сервиса, либо проходить аутентификацию через приложение.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Лисовицкий Денис Владимирович
магистрант
Таврическая академия, факультет математики и информатики
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СЕТЕВАЯ БЕЗОПАСНОСТЬ

В век информационных технологий сетевая безопасность является одной из важнейших проблем. Подавляющему большинству организаций необходимо предоставлять безопасный доступ для своих сотрудников к сетевым ресурсам для эффективной работы, из-за чего присутствует постоянная угроза хищения личных и корпоративных данных. В этой связи обеспечение сетевой безопасности одна из приоритетных задач, которая должна обеспечивать эффективное управление сетью, её безопасность и защиту от различных, постоянно развивающихся, способов атак. Проблема обеспечения сетевой безопасности усложняется с течением времени, т.к. современные работники, использующие различны персональные устройства (телефоны, ноутбуки), создают новые проблемы для безопасности сетей.

В настоящее время все большую популярность набирают беспроводные сети (wi-fi), по причине большего удобства в установке и использовании, обеспечение безопасности в некоторых случаях отходит на второй план. Рассмотрим некоторые из защитных протоколов wi-fi сетей их преимущества и недостатки:

- WEP (Wired Equivalent Privacy) - протокол для обеспечения безопасности сетей Wi-Fi, использующий ключи длинной 40, либо 104 бита что есть крайне короткая комбинация и подобрать её можно за секунды, т.к. был придуман в 90-е, в настоящее время сетей использующих эту защиту все меньше.
- WPS (QSS) - протокол автоматически обозначает имя сети и задает шифрование, для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры. Однако из-за ошибки в стандарте для взлома нужно угадать 4 цифры из 8-символьного кода, состоящему из цифр, следовательно, подобрать PIN-код для подключения можно за несколько часов.
- WPA и WPA2 (Wi-Fi Protected Access) – протокол защиты, пришедший на смену WEP, обладает усиленной системой безопасности данных и ужесточённый контролем доступа к беспроводным сетям. Длина пароля — произвольная, от 8 до 63 байт, что сильно затрудняет его подбор. Одна из наиболее эффективных и распространенных систем защиты, но не идеальна, т.к. в общем доступе существует несколько сложных, но возможных путей её взлома.

Обеспечение сетевой безопасности становиться все более острой проблемой как для различных компаний, так и для обычных людей. По причине того, что современные протоколы защиты не могут полностью удовлетворить потребности в защите частной информации пользователей сетей, может возникать множество конфликтных ситуаций, что приводит к различным негативным социальны последствиям.

УДК 004.056.53

Левоневский Дмитрий Константинович
младший научный сотрудник
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук (СПИИРАН)
Санкт-Петербург, Россия

ПРАКТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ СЕТЕВЫХ ПРОТОКОЛОВ ПРИКЛАДНОГО УРОВНЯ

Стремление к созданию единой, универсальной и открытой для изменений структуры компьютерных сетей привело к тому, что Международная организация по стандартизации (ISO) предложила концепцию открытых систем. Использование этой концепции нашло применение в стандартной модели взаимодействия открытых систем ISO/OSI, разработанной в начале 1980-х годов и ставшей в дальнейшем основой для современного стека протоколов TCP/IP. Модель OSI определяет различные уровни взаимодействия систем, а также функции, выполняемые каждым уровнем. Часть открытой системы, реализующая некоторую функцию и входящая в состав того или иного уровня, называется объектом. Набор правил взаимодействия объектов одного и того же уровня называется протоколом этого уровня.

Прикладной уровень объединяет приложения, построенные на клиент-серверной архитектуре. К ним относят протоколы удалённого управления (Telnet, SSH), передачи данных (FTP, HTTP), управления электронной почтой (SMTP, IMAP, POP3), управления доменными именами (DNS), и многие другие. Необходимость обеспечения безопасности всех этих служб трудно переоценить.

Проблемы безопасности прикладных протоколов можно разделить на группы:

- проблемы, связанные с передачей данных;
- проблемы, связанные с клиентским программным обеспечением;
- проблемы, связанные с серверным программным обеспечением.

Многие классические протоколы (HTTP, FTP, Telnet, почтовые протоколы) используют текстовые команды, передаваемые по сети в открытом виде. В этих случаях каждый запрос проходит через множество сетей, любая из которых может быть

использована для прослушивания или вмешательства в соединение. Кроме этого, существует множество дополнительных угроз, зависимых от специфики конкретного протокола: недостаточная аутентификация, предсказуемые значения идентификаторов, злоупотребление функциональными возможностями и т.п.

TLS (Transport Layer Security) - протокол, наиболее часто применяемый для обеспечения безопасных клиент-серверных соединений. Протокол TLS предназначен для предоставления трёх услуг всем приложениям, работающим над ним, а именно: шифрование, аутентификацию и целостность. TLS использует:

- асимметричную криптографию для аутентификации;
- симметричное шифрование для конфиденциальности;
- коды аутентичности сообщений (имитовставку) для контроля целостности данных.

Современные защищённые прикладные протоколы, как правило, строятся на базе TLS. Самым очевидным решением является использование незащищённого прикладного протокола поверх TLS – так работают протоколы HTTPS и FTPS. Эти технологии широко распространены, но без понимания принципов их работы эффект может быть сведён к нулю из-за наличия отдельных небезопасных элементов системы. Кроме того, существуют уязвимости, связанные с конкретными реализациями протокола (например, атака Logjam).

Другой широко используемый подход к защите передачи данных на прикладном уровне основан на протоколе SSH. Уже давно существуют технологии rsh (Remote Shell), rlogin, telnet, позволяющие определённым пользователям определённых компьютеров работать с командной оболочкой другого компьютера. Эти технологии уязвимы к перехвату, спуфингу, модификации данных. В результате задача организации безопасного доступа к удалённой консоли была решена с помощью протокола SSH (Secure Shell).

В настоящее время, когда сетевые технологии используются для управления сложными технологическими объектами, денежными потоками, конфиденциальными данными, а сбои в работе прикладных приложений или сетевой инфраструктуры могут привести к катастрофам и огромным убыткам, значение технологий защиты сетей трудно переоценить. Защищённые прикладные протоколы значительно повышают безопасность информационных систем, но при этом необходимо понимать базовые принципы реализации этих протоколов и ограничения в их применении. Защищённый сетевой протокол позволяет контролировать подлинность агентов, целостность и конфиденциальность данных, но не убережёт от уязвимостей в клиентских и серверных приложениях и от вредоносного программного обеспечения. Поэтому необходимо понимать, что только комплексный подход к обеспечению защиты информации, где защищённые прикладные протоколы – только одно из используемых средств защиты, обеспечит приемлемый уровень рисков.

Литература

1. Стандарт: ISO 15408 - Общие критерии оценки безопасности информационных технологий.
2. Модель OSI [Электронный ресурс]. URL: http://www.citforum.ru/nets/switche/ osi.shtml.
3. Стандарт: RFC 793. Transmission Control Protocol.
4. Стандарт: RFC 2246. The TLS Protocol Version 1.0.
5. Стандарт: RFC 2616. Hypertext Transfer Protocol – HTTP/1.1.
6. Стандарт: RFC 959. File Transfer Protocol (FTP).
7. Стандарт: RFC 4217. Securing FTP with TLS.
8. Стандарт: RFC 4251. The Secure Shell (SSH) Protocol Architecture.
9. Стандарт: RFC 2821, RFC 2822. Simple Mail Transfer Protocol.
10. Стандарт: RFC 3501. Internet Message Access Protocol - Version 4rev1.
11. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2010. – 958 с.
12. Что такое TLS [Электронный ресурс]. URL: http://habrahabr.ru/post/258285/
13. Уязвимость FREAK в TLS/SSL – Хакер. [Электронный ресурс]. URL: https://xakep.ru/2015/03/04/freak/
14. Венедюхин А. Ключи, шифры, сообщения: как работает TLS. [Электронный ресурс]. URL: https://tls.dxdt.ru/tls.html
15. Воробьев В.И., Рыжков С.Р., Фаткиева Р.Р. Защита периметра в облачных вычислениях. Третий национальный суперкомпьютерный форум (НСКФ-2014) Переславль-Залесский 25-27 ноября 2014 г. http://www.nscf.ru/materialy-foruma/

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Курочка Дмитрий Николаевич
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭТАПОВ ИННОВАЦИЙ

Инновационное развитие является приоритетным направлением во всех развитых и развивающихся странах, но реализация его происходит по различным сценариям, с различными темпами и масштабами, но всюду инновации проходят одинаковый путь от возникновения до выпуска. Этапами создания и реализацией инноваций можно назвать следующие: 1) возникновение новой идеи, представляющей коммерческую и научную ценность; 2) разработка технологии на основе данной идеи; 3) создание опытного образца, испытание и усовершенствование; 4) внедрение технологии для производства опытной (пилотной) партии товаров; 5) распространение технологии, копирование инновационного продукта – диффузия инновации. На перечисленных этапах происходит также поиск инвестора, партнеров по производству и сбыту и другие Действия, которые необходимы для выпуска любого продукта. На каждом из перечисленных этапов необходима информационная защита, позволяющая сначала автору идеи, а затем и производителю нового товара предотвратить хищение технологий и других предметов интеллектуальной собственности. На первом этапе, даже после достаточно четкой формулировки новой научной или технической мысли, бывает достаточно сложно оценить ее с позиций практического применения, поэтому даже публикация в открытой печати способна закрепить авторство. Но такая фиксация интеллектуальной собственности не гарантирует, что, во-первых, высказанная мысль не будет затем несколько отредактирован и присвоена другим человеком, и, во-вторых, что на ее основе могут быстрее разработать инновационную технологию, чем это сделает производитель, которому автор передаст свою идею. К сожалению, процесс официального патентования является достаточно сложным и нет гарантии, что по его завершению уже будет выпущен аналогичный продукт другой фирмой. Примером отрицательного результата опубликования многочисленных новаторских идей является журнал «наука и жизнь», в котором советские граждане делились «маленькими хитростями» (так называлась рубрика журнала с рисунками, схемами и краткими описаниями устройств и бытовых приспособлений), которые с успехом и без всяких объяснений были запатентованы в Японии. Даже персонаж Чебурашка стал по праву японским, т.к. не был оформлен в России с точки зрения авторского права. Многие исследователи, прежде, чем опубликовать научную статью, сначала патентуют ее, получая регистрационный номер, а затем уже с изменениями, дополнениями и пояснениями передают в редакцию некоторого издания. Такой же прием можно использовать на других этапах разработки инновации, касается она физического объекта, названия (бренда), технологии, вида опытного образца и его «начинки» - все описания, рисунки, фотографии представляют собой информацию, которую автор (или организация) должны прежде всего зафиксировать в соответствующих формах и получить подтверждающие документы.

Само производство инновационного продукта также содержит ряд этапов, относящихся к технологическому процессу и к сопровождению производства, планированию и диспетчеризации [1]. К первому блоку относятся нормирование материалов и трудоемкости, организация и управление инструментальным хозяйством, развитие специализации и кооперации производства; ко второму – создание нестандартного оборудования, обновление и развитие основных производственных фондов, совершенствование логистики. На каждом из данных этапов и их компонент могут возникнуть различные технологические и управленческие инновации,

составляющие знания данной организации и также подлежащие фиксированию, хранению и правовому закреплению.

Литература

1. Федоров В.К., Бендерский Г.П., Епанешникова И.К. О теоретических и методологических подходах к построению систем управления инновациями // Методы менеджмента качества**.** 2009. № 5**.** С. 25-29.

УДК 004.056.57

Бойченко Олег Валерьевич
д.т.н., профессор
Петриченко Виталий Игоревич
студент 4 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЗАДАЧИ ПРИМЕНЕНИЯ СИТУАЦИОННЫХ ЦЕНТРОВ В УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

Ситуационные центры в последние годы находят все большее применение в сфере принятия обоснованных решений для сложных аналитических задач. Они эффективно используются для управления ресурсами компаний и регионов, ускорения подготовки управленческих решений и в других областях.

Обычно российскими разработчиками ситуационная комната рассматривается как интеллектуальная вершина, в которую поступает множество сообщений по каналам связи, а группа людей, сидящая в комнате, - как некий супермозг, который всю эту информацию впитывает и перерабатывает.

При таком подходе, конечно, допустимы и интерактивные процессы. Они приемлемы для организации мониторинга, исследования детерминированной сферы, разрешения некоторых чрезвычайных ситуаций. В любом случае эффективность использования ситуационной комнаты здесь связана с максимизацией мультимедийных средств и коммуникационных каналов.

Следует отметить, что некоторые современные тенденции в развитии методологических подходов к проектированию ситуационных комнат переходят к новым приоритетам:

- от точности к интеллектуальности;
- от справочной работы к аналитической;
- от одного эксперта к группе;
- от внутренней среды к внешней;
- от инерционной экстраполяции к поиску новых путей;
- от регистрации данных к экстракции знаний;
- от защиты информации к менеджменту безопасности;
- от накопления опыта к когнитивным схемам.

Создание ситуационных центров (СЦ) является сегодня одной из актуальнейших задач повышения эффективности управленческой деятельности. В настоящее время в мире насчитывается несколько сотен ситуационных центров, и количество их продолжает увеличиваться. Достаточно активно сегодня ситуационные центры начинают внедряться и в образовании. Это действительно эффективная форма передачи знаний. Сегодня знания, кадры, специалисты - актуальнейшее условие, оно будет определять в ближайшее время развитие всех сфер деятельности в нашей стране.

Важнейшими факторами, обеспечивающими активное внедрение СЦ в практическую деятельность органов управления, являются:

- необходимость совершенствования управленческих процедур путем включения в них руководства не только на этапе принятия, но и выработки решения;

- возможность оптимизации принимаемых решений путем их экспертной оценки и моделирования ситуации с помощью современных информационных технологий;
- возможность повышения качества предварительного анализа информации и вырабатываемого решения путем использования современных информационных технологий, обеспечивающих интеграцию средств связи, аналитической обработки и визуализации информации;
- необходимость обеспечения лиц, вырабатывающих и принимающих решения, достоверной полной информацией по проблеме;
- возможность оперативного доступа первого лица ко всей информации, относящейся к вопросу, требующему решения.

В заключении отметим, что под принятием решения обычно понимается не отдельный акт выбора одного из некоторых готовых решений, а многоэтапный процесс, имеющий сложную динамическую структуру. Поэтому в решении отражается все то ценное, что было получено в процессе предшествующей информационно-аналитической деятельности. Существенное влияние на повышение качества принимаемых решений оказывает использование современных технологий принятия решений, в которых далеко не последняя роль отводится использованию различных методов экспертного оценивания.

УДК 001.895

Герасимова Светлана Васильевна
д.э.н., профессор
Трофимов Артём Сергеевич
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ ИННОВАЦИОННЫХ ПРОЦЕССОВ ПРЕДПРИЯТИЯ

В настоящее время, все предприятия стремятся к получению уникальных преимуществ над своими конкурентами. Для этого они применяют новые методы управления или создают новый продукт. Но, в любом случае, получение преимуществ связано с применением инноваций, так как именно они помогут достигнуть желаемого результата.

Инновация – это ввод новых продуктов. Инновации решают потребительскую проблему или удовлетворяют потребность, для которой ранее не было товаров. Инновационный процесс предполагает развитие функционирования хозяйства на качественно новом уровне.

Наиболее точно характеризует понятие «инновация» следующее определение: «Инновация (нововведение) – это конечный результат творческой деятельности, получивший воплощение в виде новой или усовершенствованной продукции, реализуемой на рынке, либо нового или усовершенствованного технологического процесса, используемого в практической деятельности» [3, с. 11]. То есть инновацией является результат внедрения новых идей и знаний, который необходим для удовлетворения запросов потребителей.

Следовательно, инновация – это конечный результат с определенным началом, где стартом является новая идея или изобретение. Для того, чтобы эта идея осуществилась, ей необходимо пройти множество этапов и действий. Именно эти этапы и действия в совокупности характеризуют инновационный процесс.

Инновационный процесс – это процесс, направленный на разработку и реализацию результатов законченных научных исследований и научно-технических достижений в

виде нового или усовершенствованного продукта, реализуемого на рынке, нового или усовершенствованного технологического процесса, используемого в практической деятельности [4, с. 15].

Согласно теории нововведений Й.А. Шумпетера, диффузия нововведения является процессом кумулятивного увеличения числа имитаторов, внедряющих новшество вслед за новатором в ожидании более высокой прибыли. Период, который начинается с выполнения теоретических исследований, а заканчивается моментом, когда «новая» техника подлежит замене на более эффективную технику, называется жизненным циклом инновации. Таким образом, жизненный цикл инновации включает в себя: этап возникновения потребности в новшестве и его создание (приобретение прав на использование новшества у его владельца); этап освоения в производстве; этап диффузии (тиражирования на других объектах); этап рутинизации (стабильное, без изменения, использование) [1, с. 312].

Важной особенностью осуществления инновационных процессов в производстве является преобладающее значение знаний, необходимых для реализации данных процессов. Соответствующие знания оказывают огромное влияние на эффективность процесса производства товаров, модернизацию технологий, создание новых производств, развитие информационных технологий, повышение уровня наукоемкого производства.

В настоящее время организация должна осуществлять непрерывные инновационные процессы. Для того чтобы внедрять инновации в постоянном режиме, необходимо обладать соответствующими знаниями. Управление знаниями – одна из ключевых составляющих управления процессом инноваций. Нестабильные условия внешней среды вынуждают организации принимать на вооружение знания, созданные вне организации поставщиками, покупателями, продавцами, государственными структурами и конкурентами.

Значимую роль при введении инновации играют иностранные инвестиции. Прямые иностранные инвестиции обеспечивают конкурентоспособность и экономический рост не только предприятия, но и страны в целом. Иностранные инвесторы здесь выступают не только в качестве источника финансирования, но и как «прародитель» более высоких технологий в производстве, менеджменте и других областях. Но сейчас иностранные инвестиции трудно внедрить в экономический процесс, так как нет благоприятного инвестиционного климата из-за политической и экономической нестабильности в стране. Но «если темп прироста выручки от инновационных проектов выше темпов прироста инфляции, наблюдается рост внедрения инноваций в производство» [2, с. 110].

Следующей особенностью инновационных процессов в производстве является бенчмаркинг, представляющий собою искусство выявлять то, что другие предприятия делают лучше, а также изучение их методов работы. В основу бенчмаркинга положена идея сравнения деятельности не только предприятий – конкурентов отдельного региона, но и передовых организаций других регионов. Практика показывает, что грамотное использование опыта конкурентов и успешных компаний позволяет сократить затраты, повысить прибыль и оптимизировать выбор стратегии деятельности данных организаций.

Другой немаловажной особенностью инновационных процессов в производстве является интрапренерство (развитие духа предпринимательства и его осуществление внутри существующих предприятий). Сущность интрапренерства заключается в том, что на определенном предприятии, которое выпускает продукт или услугу, создаются условия для выдвижения новаторских идей, выделяются ресурсы для реализации и оказывается помощь для их практического использования [5]. Цель интрапренерства – повышение эффективности предприятия за счёт использования творческого потенциала работников, быстрая реакция на изменение потребностей рынка и всевозможных нововведений.

Чтобы достигнуть высоких результатов в инновационной сфере, важно стимулировать труд работников, занятых в этой сфере. Общеизвестными факторами

мотивации являются нормальные условия труда, достаточная заработная плата, уважительное отношение администрации и др. [4, с. 78-79]. Можно выделить следующие способы стимулирования труда в инновационной сфере: участие в прибылях от использования новшества; уровень текущей заработной платы работников занятых в сфере инновационных технологий должен быть несколько выше, чем в среднем по организации; обеспечение возможности проведения исследования в интересующей исследователя области; гибкий режим рабочего дня; возможность совмещения научного роста и продвижения по служебной лестнице [4, с. 80-81].

Наиболее выгодный метод для поэтапного создания старта для инноваций – это управление сопротивлением, но его сложность заключается в планировании и организации. Осуществление плана введения инноваций и их проведение является сложной задачей. Возникает сопротивление персонала, негативно отражающееся на сроках проведения инноваций. Чтобы преодолеть такие проблемы нужно иметь огромный опыт в сфере управления предприятием и иметь соответствующие ресурсы. Обычно, чтобы организовать такой инновационный проект приглашается на предприятие консультант, который разрабатывает план введения изменений.

После внедрения инновации в производство важно засвидетельствовать или запатентовать товар или услугу. Для каждого объекта собственности существуют различные формы защиты [4, с. 104]: патент, свидетельство или ноу-хау (конфиденциальные знания, которые не являются общеизвестными). Существует авторское право, которое распространяется на произведения, которые являются результатом творчества. Оно пожизненно принадлежит автору и существует еще 50 лет после его смерти. Патент же является официальным документом, который подтверждает право владельца на объект. Патенты выдаются на технические и художественно-конструкторские решения, т.е. описывающие конкретные материальные объекты (машины, механизмы, различные устройства, составы, смеси и т.д.), в то время как свидетельства выдаются на объекты, относящиеся к творческим произведениям, т.е. изобразительным, фантазийным объектам, таким как художественные изображения [4, с. 108]. Существует также товарный знак – бренд или просто фирменное наименование.

Таким образом, инновационные процессы предприятия – это процессы преобразования научного знания в нововведение, которые представляются как последовательная цепь действий, в ходе которых нововведение созревает от идеи до конкретного продукта, технологии или услуги и распространяется на практике. Рассмотрев особенности инновационного процесса предприятия, можно сделать вывод, что одним из самых эффективных улучшений работы предприятия в нашей стране является бенчмаркинг (метод поиска и внедрения наиболее успешных инноваций на всех уровнях предприятия с целью увеличения его конкурентоспособности). Однако, не менее важным фактором в особенностях инновационных процессов является мотивация работников предприятия различными способами, что способствует внедрению интрапренерства.

Список использованной литературы:

1. Базилевич В. Д. Неортодаксальная теория Й. А. Шумпетера // История экономических учений: В 2 ч. — 3-е издание. — К.: Знання, 2006. — Т. 2. — 575 с.
2. Бакланов А.О., Диденко Н.И. Роль инноваций в мировых процессах экономического роста и развития / А.О. Бакланов, Н.И. Диденко. СПб.: Изд-во Политехн. ун-та, 2007. – 414 с.
3. Воронина Т.П. / Инновационный менеджмент: Учебник для вузов / Абрамешин А.Е., Воронина Т.П., Молчанова О.П., Тихонова Е.А., Шленов Ю.В.; Под редакцией д-ра экон. наук, проф. О.П. Молчановой. - М.: Вита-Пресс, 2001. - 272 с.
4. Степанова И.П. Инновационный менеджмент / Инновационный менеджмент: курс лекций для студентов, обучающихся по направлению подготовки 080200.62 «Ме- неджмент» (профиль «Менеджмент организации») / Саратовский социально-экономический институт (филиал) ФГБОУ ВПО «РЭУ им. Г.В. Плеханова». – Саратов, 2014. – 124 с.
5. Томилов В.В., Крупанин А.А., Хакунов Т.Д. Маркетинг и интрапренерство в системе предпринимательства: Учеб. пособие / В.В. Томилов, А.А. Крупанин, Т.Д. Хакунов. – СПб.: Изд-во СПбГУЭФ, 2008. – 130 с. / [Электронный ресурс]: http://www.marketing.spb.ru/read/m20/

Дюличева Юлия Юрьевна
к.ф.-м.н., доцент
Таврическая академия
Мулюкбаева Виктория Юрьевна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И.Вернадского»
Симферополь, Республика Крым, Россия

ВНЕДРЕНИЕ СИСТЕМ БИЗНЕС-АНАЛИТИКИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для обеспечения конкурентоспособности в современных условиях любая крупная компания должна внедрять системы информационной безопасности (например, системы защиты от утечек информации, наблюдения за действиями пользователей, анализа незащищённых каналов передачи информации и другие). Количество информации в корпоративных информационных системах стремительно растет в процессе работы, что приводит не только к необходимости её фильтрации и обработки, но и к решению задач защиты конфиденциальной информации. Новым подходом к анализу и защите информации является использование технологии Business Intelligence (BI), расширяющей, в общем случае, подходы к решению задач бизнес-аналитики.

Business Intelligence – это способы и инструменты для преобразования необработанной информации в осмысленную, восприимчивую форму. Технология BI позволяет обрабатывать огромные объемы неупорядоченной информации с целью поиска новых стратегических возможностей для развития бизнеса [2].

Цель технологии BI – интерпретация больших объемов информации с выделением значимых показателей, разработкой имитаций действий и анализом принятых решений.

С помощью BI-систем, которые используются в бизнес-анализе и информационной безопасности, становится возможным упорядочение больших объемов информации из разнообразных источников, дальнейшая их фильтрация и анализ выявленных закономерностей. Итоги анализа представляются в виде наглядных докладов, при помощи которых можно быстро отыскать проблемы, определить их первоисточники, а затем принять решения. Кроме того, на основании отчетности BI-системы позволяют создавать разнообразные срезы данных, исходя из вида аналитических задач.

Внедрение технологии BI для обеспечения информационной безопасности даёт возможность контролировать данные и состояние безопасности в режиме онлайн, наглядно видеть деятельность по обеспечению информационной безопасности в динамике и увеличивать эффективность принятия управленческих решений.

Рассмотрим наиболее популярные сервисы, реализованные на основе технологии BI.

1. QlikView – это наиболее популярная платформа среди платформ бизнес-аналитики, сочетающая в себе такие характеристики как небольшой срок внедрения, оптимальную стоимость, применение современных способов анализа и представления данных, простоту и работу на мобильных устройствах [2].

2.Microsoft Power BI — это комплект веб-служб и функций, с помощью которых можно находить и представлять данные в наглядном виде, делиться найденной информацией и совместно работать над анализом данных.Power BI — это улучшенное сочетание нескольких ранее популярных товаров: Data Explorer, GeoFlow, BI Sites и мобильных технологий.

3.SQL Server Reporting Services (SSRS) —программа составления отчётов, которая реализована компанией Microsoft. Её применяют для подготовки большого количества печатных отчётов и отчётов в формате онлайн. Система управляется через веб-интерфейс.

Список использованной литературы
1.Сайт Информационная безопасность [Электронный ресурс] – Режим доступа: http://www.itsec.ru/articles2/Oborandteh/business-intelligent-dlya-informatsionnoy-bezopasnosti#sthash.PKoOByH3.dpuf
2. Сайт comparex-group retail [Электронный ресурс] – Режим доступа: http://www.comparex-group.com/web/ru/ru/konsalting-i-servisy/avtomatizacija-processov-IT/BI/BI.htm

УДК 338.45 : 004.35

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Соколовская Валерия Олеговна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

3-D ПЕЧАТЬ – НОВАЯ ТЕХНОЛОГИЯ, НОВАЯ ОПАСНОСТЬ

Через несколько коротких лет 3-D принтер может стать для нас вполне обыденной и привычной вещью.

Не углубляясь в саму технологию 3-D печати, отметим, что с ее помощью можно создавать детали и объекты по заданным в компьютере параметрам. Данная технология может активно использоваться в производстве, медицине, а также пользователями в повседневной жизни, в целом, перспектива огромна.

Однако всегда найдутся те, кто сумеет использовать инновацию во вред обществу. Ярким примером является возможность печати огнестрельного оружия. Так, настоящей сенсацией стало появление в сети файла со схемами пистолета под названием «Liberator», предназначенного для создания на 3D-принтере. Суть такого применения 3-D принтера заключается в том, что все детали (исключая пулю) получаются путем использования технологии 3-D печати. Интересно то, что способ скачивания файлов был таковым, при котором файлообменник кодировал все данные о его посетителях. На данный момент, по просьбе властей, материалы изъяты из публичного доступа.

Все же, нельзя оставить без внимания, те данные, которые были распространены. Информация была удалена, но точно неизвестно, какая часть пользователей успела ознакомиться с ней. Эта информация может, в недалеком будущем, появится на различных файлообменниках, что поспособствует ее массовому распространению.

На данный момент 3-D принтер является относительно дорогостоящим оборудованием (цены варьируются от 200$ до 11000$), но в тоже время достаточно доступным, то есть, вполне возможно сделать себе пластиковое, полностью функциональное оружие, в домашних условиях, которое, к тому же, невозможно обнаружить металлоискателем.

Отходя от темы создания оружия, отметим, что 3-D принтер может стать причиной промышленного переворота, который бросит вызов настоящей модели авторского права.

Если уже сегодня ситуация представляет угрозу для авторского права (скачивание музыки, книг и т.д. с торрентов), что же будет, когда любой желающий сможет распечатать понравившуюся вещь просто у себя дома.

Данный вопрос был задан Майклу Вайнбергу (юрист, в области информационных технологий). Он заявил, что защите авторских прав подлежат те предметы, которые выполняют чисто эстетическую функцию. Если же с помощью этого предмета можно что-либо делать, то он не подлежит защите. Т.е., при создании, например, столов и стульев закон не будет нарушен.

Если настоящий закон об авторском праве не будет дополнен, то вскоре, будет полностью игнорироваться.

Нельзя не отметить возможность угрозы перехвата и подмены информации в сети Интернет, ведь это может нести в себе не только финансовые риски, но и представлять собой оружие массового уничтожения.

Технология 3-D печати несет в себе как большие преимущества для человечества в различных сферах деятельности, так и опасность. Понятно, что после укоренения в нашей жизни 3–D принтера, произойдет значительное изменение логистики промышленности. Это может, как положительно модернизировать наш мир, так и привести к значительным последствиям, как финансовым так и, в целом, опасным для жизни.

УДК 004.42

Мокрицкий Вадим Андреевич
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

К ВОПРОСУ О МЕТОДАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

Рассмотрены применимости моделей доступа для системы информационной безопасности геоинформационных систем. Проанализированы основные модели доступа, применяемые при проектировании и создании современных автоматизированных геоинформационных систем.

Ключевые слова: *геоинформационные системы, ГИС, методы защиты.*

Геоинформационная система (ГИС)– совокупность технических, программных и информационных средств, обеспечивающих ввод, хранение, обработку математико-картографическое моделирование и образное интегрированное представление географических и соотнесенных с ними атрибутивных данных для решения проблем территориального планирования и управления.

Преимущества ГИС перед другими информационными технологиями:

- наличие набора средств создания и объединения баз данных;
- обеспечение географического анализа и наглядной визуализации БД в виде различных карт, графиков, диаграмм;
- возможность прямой привязки друг к другу в режиме «горячая ссылка» всех атрибутивных и графических данных.

Сфера применения ГИС в бизнесе охватывает разные области, такие как:

- анализ и отслеживание текущего состояния и тенденций изменения рынка;
- планирование деловой активности;
- оптимальный выбор местоположения новых филиалов фирмы или банка, торговых точек, складов, производственных мощностей;
- поддержка принятия решений;
- выбор кратчайших или наиболее безопасных маршрутов перевозок и путей распределения продукции;
- анализ риска материальных вложений и урегулирование разногласий;
- демографические исследования, проводимые в целях определения спроса на продукцию;
- географическая привязка баз данных о земле- и домовладении.

Некоторые задачи решаемые геоинформационной системой в разрезе определенного населенного пункта или региона, а так же в глобальном масштабе:

1. быстро выявить по карте, где скрываются покупатели и конкуренты;
2. определить наиболее выгодное для бизнеса местоположение новых производственных мощностей, филиалов и торговых точек;

3. составить сводные диаграммы объемов продаж за месяц или год по интересующим торговым предприятиям и их расположением;

4. визуально оценить и получить полноценную статистическую сводку по динамике спроса и предложения в любой области рынка и рассматриваемой территории, например в операциях с недвижимостью;

5. визуально по карте и на основе сопутствующей цифровой и текстовой информации провести сравнение демографических характеристик по разным странам, областям и районам;

6. выявить и оконтурить неблагополучные по экологическим признакам районы или зоны повышенной чувствительности природной среды к антропогенным воздействиям;

7. нанести на карту, выделить и дополнить сопутствующей информацией зоны производства, хранения, сброса и накопления вредных для людей и живых организмов веществ и материалов.

Построение современных геоинформационных систем (ГИС), доступ к последним через компьютерные сети и сети Internet тесно связано с проблемой обеспечения информационной безопасности. Наличие большого количества данных карты, как основной формы представления информации, разнообразие решаемых с его помощью производственных и иных задач, широкий круг потенциальных его пользователей заставляют особенно тщательно относиться к решению данной задачи. Одним из основных моментов, определяющих ее успешное решение, является применение формальных моделей безопасности на всех этапах жизненного цикла системы, особенно на этапе проектирования. При этом наиболее важным является использование формальных моделей при проектировании систем контроля и управления доступом.

Формальные модели безопасности играют важную роль в процессах проектирования, разработки, сертификации и исследования защищенной ГИС, так как обеспечивают системотехнический подход, включающий решение такой задачи, как выбор и обоснование базовых принципов архитектуры защищенной ГИС, определяющих механизмы реализации средств и методов защиты информации от несанкционированного доступа.

Среди формальных моделей безопасности выделяют модели управления доступом. Модели этого класса предназначены для обеспечения решения задач анализа и синтеза систем (механизмов) разграничения доступа к различным видам ресурсов ГИС.

Модели управления доступом определяют правила управления доступом к информации, разрешениями в системе таким образом, чтобы система всегда была безопасна.

Основными формальными моделями управления доступом, используемыми в современных компьютерных системах, являются дискреционные, мандатные и ролевые модели. Рассмотрим модели безопасности, используемые в настоящее.

При создании механизмов контроля доступа необходимо определить множество субъектов и объектов доступа. Субъектами могут быть пользователи, процессы и процедуры. Объекты: файлы, программы, директории, терминалы, каналы связи, устройства и т.д. Субъекты могут одновременно рассматриваться и как объекты, поэтому у субъекта могут быть права на доступ к другому субъекту.

При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности. Общим подходом для всех моделей является разделение множества сущностей, составляющих систему, на множества субъектов и объектов, хотя сами

определения понятий «объект» и «субъект» в разных моделях могут существенно различаться.

Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

Основной элемент модели безопасности - это доказательство утверждения о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Создание систем информационной безопасности в ГИС должна основываться на следующих принципах:

- системный подход, учитывающий концепцию открытых систем и интероперa-бельности;
- принцип непрерывного развития системы и непрерывности защиты;
- разделение и минимизация привилегий доступа;
- эшелонирование обороны;
- полнота контроля и регистрации попыток;
- управляемости системы защиты;
- обеспечение экономической целесообразности использования системы защиты.

Рассмотрим модели доступа управления доступом для построения системы информационной безопасности ГИС

Дискреционные модели реализуют дискреционное управление доступом, основанное на заданном множестве отношений доступа. Классической дискреционной моделью является модель Харрисона-Руззо-Ульмана. Система обработки информации представляется в виде совокупности активных субъектов S, пассивных объектов O и конечного множества прав доступа R={r1, …, rn}. Субъекты осуществляют доступ к информации, объекты содержат информацию, права доступа означают полномочия на выполнение соответствующих действий (чтение, запись, выполнение). Еще одним моментом является то, что все субъекты являются одновременно и объектами, это позволяет представлять права доступа между субъектами $S \subset O$.

Поведение системы моделируется с помощью понятия «состояния». Пространство состояний системы образуется декартовым произведением множеств составляющих ее объектов, субъектов и прав. Текущее состояние системы Q в этом пространстве определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа M, описывающей текущие права доступа субъектов к объектам, - Q = (S, O, M). Строки матрицы соответствуют субъектам, а столбцы - объектам, поскольку множество объектов включает в себя множество субъектов, матрица имеет вид прямоугольника. Любая ячейка матрицы M[s, o] содержит набор прав субъекта S к объекту O,

принадлежащих множеству прав доступа R.

Особо важным то, что с точки зрения практики построения систем информационной безопасности модель Харрисона-Руззо-Ульмана является наиболее простой в реализации и эффективной в управлении, поскольку не требует никаких сложных алгоритмов и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее широкая распространённость среди современных систем. Кроме того, предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия.

Для систем информационной безопасности, ориентированной на работу в среде интернет/интранет применение дискреционной модели является недостаточно эффективным. Это касается уязвимости моделей, связанным с особенностями информационных систем, в которых используются большое число объектов и субъектов доступа, таких как ГИС крупного промышленного предприятия, инженерные сети которых содержат десятки тысяч отдельных объектов, администрирование системы является достаточно трудоемкой задачей.

Кроме того, все дискреционные модели уязвимы по отношению к атаке с помощью «троянского коня», поскольку в них контролируются только операции доступа субъектов к объектам, а не потоки информации между ними.

Мандатные модели реализуют мандатное управление доступом, которое основано на совокупности правил, определенных на множестве атрибутов безопасности субъектов и объектов. Основой мандатных моделей является модель Белла-ЛаПадулы, базирующаяся на правилах секретного документооборота. На основе текущей политики безопасности в модели Белла-ЛаПадулы каждому субъекту и каждому объекту назначаются собственные уровни секретности. Уровни секретности образуют иерархию от самого высокого до самого низкого. Для предоставления доступа к объекту уровень секретности субъекта сравнивается с уровнем секретности объекта. В модели Белла-ЛаПадулы под безопасностью понимается такое состояние системы, при котором обеспечивается конфиденциальность информации, то есть такое состояние системы (субъектов и объектов), при котором исключается несанкционированный доступ. В качестве входных воздействий на систему выступают операции доступа субъектов «читать» и «записывать»:

1) уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности;

2) уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

В результате этих воздействий система может переходить как в безопасные состояния, так и в небезопасные. Например, если в результате выполнения какой-либо операции данные становятся доступными для субъектов с более низким допуском (стал возможен несанкционированный доступ), то это означает, что система перешла в небезопасное состояние.

Все мандатные модели, как и модель Белла-ЛаПадулы, используют только два права доступа - чтение и запись. На практике информационные системы поддерживают значительно более широкий спектр операций над информацией, например: создание, удаление, передача и т.д. Следовательно, для того чтобы применить мандатную модель к реальной системе, необходимо установить подходящее соответствие между чтением и записью и операциями, реализованными в конкретной системе. Определение такого соответствия представляет собой нетривиальную задачу, поскольку в реальной жизни

невозможно ограничиться однонаправленными потоками информации, идущими строго от субъекта к объекту или наоборот.

В *ролевой модели* операции, которые необходимо выполнять в рамках какой-либо служебной обязанности пользователя системы, группируются в набор, называемый «ролью».

Классическое понятие «субъект» в ролевой модели замещается понятиями «пользователь» и «роль». Пользователь - это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль - это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления определенной деятельности.

При использовании ролевой политики управление доступом осуществляется в две стадии:

1) для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам;

2)каждому пользователю назначается список доступных ему ролей.

Например, операции по регистрации документов могут быть сгруппированы в роль «регистратор». Для того чтобы множества операций, связанных с различными ролями, не пересекались, вводится иерархическая зависимость между ролями. К примеру, роль «секретарь» может включать в себя роль «регистратор» и, плюс к тому, еще несколько дополнительных операций. Каждый пользователь системы играет в ней одну или несколько ролей. Выполнение пользователем определенного действия разрешено, если в наборе его ролей есть нужная, и запрещено, если есть нежелательная.

В этой модели у объектов нет определенных хозяев. Вся информация расценивается как принадлежащая организации, владеющей системой. Соответственно, и роли пользователя внутри системы – это роли, которые он играет в данной организации. Как следствие, пользователю невозможно делегировать права на какой-то определенный объект. Либо у него есть доступ ко всем подобным объектам системы, либо нет. Таким образом, преимуществом ролевой модели перед дискреционной является простота администрирования: назначение пользователей на роли и создание новых ролей не составляют никаких трудностей. В то же время она не позволяет управлять разными частями системы по отдельности, и тем более – делегировать какому-либо пользователю такие полномочия.

Ролевая политика безопасности является неотъемлемой частью современных систем управления доступом в корпоративных информационных системах со сложной организационной и штатной структурой, большим количеством пользователей, выполняющих определенные функции в рамках своих служебных обязанностей и наделенных в связи с этим различными правами и полномочиями.

Применение ролевых моделей позволяет существенно упростить проектирование и администрирование систем разграничения доступа автоматизированных информационных систем, реализующих сложные, нетривиальные организационно-технологические и организационно-управленческие схемы и процессы, присущие процессу использования и ведения геоинформационных систем.

Литература

1. Королев О.Л. Модель оценки риска кибератаки для виртуального предприятия / Королёв О.Л., Малков С.В. // Экономическая кибернетика. Международный научный журнал. - 2013. - № 1-3. - С. 80-85.

2. Марков А.С. Систематика уязвимостей и дефектов безопасности программных ресурсов / А.С.Марков и А.А.Фадин // Защита информации. Инсайд. 2013. №3. С. 56-61.

3. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография //А.А. Ссмирнов. – М.: ЮНИТИ-ДАНА:

Закон и право,
4. . Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации / И.Ю.Шахалов // Вопросы кибербезопасности. 2013. №1(1). С.49-54.
5. Ярочкин В.И. Информационная безопасность/ Учебник для вузов. 2-е издание. — М.: Академический Проект, Гаудеамус, 2004. — 544 с.

УДК 338.242.2: 004. 056. 5

Остапенко Ирина Николаевна
к.э.н., доцент
Смигельских Дмитрий Александрович
студент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

К ВОПРОСУ РЕАЛИЗАЦИИ ПРИНЦИПА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННОЙ ОРГАНИЗАЦИИ

Бурное развитие экономики в настоящее время ставит инновационную деятельность на одно из первых мест. Уровень его развития, структуры и эффективности определяют степень конкурентоспособности современных стран. Благодаря расширению инновационной деятельности государство может повысить уровень развития национальной экономики и обеспечить более высокую её конкурентоспособность на мировом рынке.

В процессе инновационной предпринимательской деятельности бизнес сталкивается с различными трудностями экономического, организационного, международного, правового, экологического плана, а также недобросовестной конкуренцией, влекущей за собой необходимость поддержания высокого уровня информационной безопасности, которая обеспечивает повышение конкурентоспособности организации на внутреннем и мировом рынках. Без надлежащей степени защиты информации применение новых продуктов может быть определено как экономически невыгодное из-за большого ущерба в связи с потерей секретных данных. В этом заключается актуальность выбранной темы в современных условиях высокой конкурентной среды.

Безопасность инновационной деятельности в предпринимательстве включает в себя защищённость субъекта предпринимательской деятельности на всех стадиях его функционирования от внешних и внутренних угроз, которые оказывают на процесс или сам объект пагубное воздействие и от попыток кражи инновационных разработок. Целью внедрения и совершенствования информационной безопасности инновационной организации является контроль по обеспечению устойчивого и эффективного функционирования инновации, обеспечение его высокого уровня конкурентоспособности. Достижение поставленной цели контроля уровня безопасности обеспечивается при выполнении следующих задач:

1) поддержание высокого уровня финансовой устойчивости и независимости инновационного предприятия;

2) обеспечение высокого уровня системы управления организацией и системы принятия управленческих решений специалистами и руководством компании;

3) разработка правовой защиты всех видов инновационной деятельности;

4) создание собственного информационного пространства предприятия, доступ к которому имеет ограниченный круг лиц и обеспечение его современными способами защиты;

5) владение информацией о финансовом положении конкурентов, их инновационных разработках, развитие мировых и отечественных тенденций в сфере инноваций и потребностей общества в новых продуктах и услугах;

6) своевременная и быстрая реакция на нарушение информационной безопасности, принятие соответствующих мер.

В аспекте изложенного, структуру защиты информации инновационной организации можно определить следующим образом (табл.1.):

Таблица 1.

Структура защиты информации

СТРУКТУРА ЗАЩИТЫ ИНФОРМАЦИИ ИННОВАЦИОННОЙ ОРГАНИЗАЦИИ					
Инженерно-техническая защита информации	Организационно-правовая защита информации	Программные средства защиты	Криптографические методы и средства	Программно-аппаратные методы и средства	Электронная подпись в условиях электронный документооборот и значение

В аспекте стратегического планирования инновационной деятельности особую роль играют инновации в сфере ИБ – генерирования и воплощения идеи по обновлению состава продуктов защиты информации [1]. Инновации в этом смысле являются необходимым условием в тех случаях, когда обновление защитных ресурсов уже не обеспечивает ИБ. Индустрия изменения профиля угроз (вирусы, хакеры, инсайдеры) диктует инновативность ИБ в рамках инновационной деятельности организации. Например, сегодня для противодействия внутренним нарушителям разрабатываются комплексные платформы безопасности - системы класса ИАС РСКД (информационно-аналитические системы режима секретности конфиденциальных данных). Риски инновационных организаций оправданы внедрением подобных инновационных решений. В данном контексте инновационность – это возможность при внедрении нового продукта или услуги максимально эффективно использовать имеющийся потенциал организации, получив конкурентные преимущества.

Информационная безопасность является неотъемлемой частью в создании, развитии и внедрении инноваций. При этом необходимо учитывать последние инновационные разработки и формировать внутрифирменную стратегию информационной безопасности, в соответствии с направлением деятельности компании. Совокупность приведенных мер создаёт условия для применения универсальной модели по обеспечению безопасности инновационной организации и создания более адекватного инструмента защиты от современных угроз.

Литература:

1. Инновации в области информационной безопасности. Оправдан ли риск? [Электронный ресурс]: Information Security/ Информационная безопасность// №2, 2009 - http://www.itsec.ru/articles2/bypub/insec-2-2009#sthash.ISe8g3OR.dpuf (дата обращения: 28.01.2016).

УДК 004.58

Пенькова Инесса Вячеславовна
д.э.н., профессор
Асанов С.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Одним из направлений любой деятельности предприятия в современном мире является использование Интернет-технологий, как для совершенствования организации различных внутренних информационных процессов, так и для развития информационных взаимодействий с поставщиками, посредниками, потребителями. Интернет-технологии предоставляют преимущества участникам процесса товарообмена.

Специалисты компании IBM выделяют ряд моделей интеграции Интернет-технологий в информационную систему предприятия (рис. 1).

Рис. 1. Классификация моделей интеграции Интернет-технологий в информационную систему предприятия [1].

Интернет-технологии зачастую являются компонентами социальных и производственных технологий. Информационные технологии (ИТ) играют ключевую роль в процессах приобретения и накопления новых знаний и данных, использование которых повышает эффективность экономических процессов.

Выполнение интернет-технологиями перечисленных функций позволяет различных предприятиям активно развиваться. При этом внедрение ИТ во внутреннее пространство компании осложнено тем, что сами по себе интернет-технологии представляются сложной комплексной системой, для отладки которой необходимы высоко квалифицированные специалисты и создание определенной технической и технологической платформы.

Формируя инновационную стратегию, ритейлеры России с повышенным интересом относятся к инновационным решениям и активно изучают возможность их применения, что позволяет анализировать и накапливать опыт инновационного развития торговли в разных странах и затем внедрять наиболее успешные из них в рамках отечественных региональных подразделений.

Список литературы

1. Иванова Е.К. Генезис применения ТИ в маркетинговой стратегии предприятия в условиях рыночных реформ в России // Менеджмент: управление в социальных и экономических системах. Сборник материалов V Международной научно практической конференции. - Пенза: РИО ПГСХА, 2011.

УДК 657.1.011.56

Чепоров Валерий Владимирович
к.ф.-м.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

DATA MINING И ИНФОРМАЦИОННЫЕ СИСТЕМЫ БУХГАЛТЕРСКОГО УЧЕТА

В простейшей итальянской системе бухгалтерского учета минимально присутствуют два документа – главный журнал (журнал хозяйственных операций), в котором отражаются транзакции по двум счетам и книга счетов, которая накапливает данные по конкретному счету. При расширении простейшей системы учета во многих информационных системах данные поступают на более высоком уровне агрегирования. В них может присутствовать лишь одна журнальная запись ежемесячно, которая охватывает все множество операций, которые были обработаны с помощью конкретной подсистемы. Например, подсистема продаж может передавать только одну запись ежемесячно, которая отражать агрегированные проводки по выручке, себестоимости проданных товаров, дебиторской задолженности и т.д. Автоматизированное извлечение информации о первоначальной сделке из главной книги, как правило, является трудоемким или невозможным в таких системах. Система главной книги, как правило,

собирает данные, которые могут возникать в различных системах обработки транзакций, в том числе подсистемах продажи, закупки, логистики, технического обслуживания и производства, при этом данные о транзакции могут поступать на различных уровнях агрегирования.

Сами по себе, главная книга (журнал хозяйственных операций) или база данных по транзакциям в бухгалтерской информационной системе является окончательным хранилищем для отражения всех экономических событий, которые влияют на организацию и, как следствие, на финансовые отчеты. Если главная книга содержит данные на уровне отдельной транзакции, то ее можно обрабатывать разными методами извлечения данных, анализа данных или применение «дата майнинга».

Data Mining (добыча данных, интеллектуальный анализ данных, глубинный анализ данных) — собирательное название, используемое для обозначения совокупности методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности. Data Mining - это процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности.

Дата майнинг фактически выполняет подобную статистической науки функцию, связанную с группированием данных. В отличие от статистики классификация в бухгалтерском учете начинается тогда, когда происходит наблюдаемое событие, которое впоследствии записывается бухгалтером. В бухгалтерском учете транзакция классифицируется тогда, когда она записывается в дебет или кредит счетов, хотя уже до этого она классифицируется как актив, обязательство, капитал, доходы или расходы. Эта классификация вытекает из фундаментального уравнения бухгалтерского учета (активы = обязательства + капитал).

Классификация счетов на основе транзакции – это группировка счетов по наиболее существенным признакам, что позволяет обеспечить единообразие в отражении хозяйственных операций, сопоставимость и сводимость соответствующих показателей. Классификация счетов дает возможность определить экономическую нагрузку каждого бухгалтерского счета. Бухгалтерская запись при предварительной классификации служит целям минимизации затрат времени для последующего анализа, предусматривающая фиксацию транзакции без последующего ее анализа. Так, если руководство компании интересуется структурой затрат по заработной плате, то в базе данных главной книги должны быть поля, связанные с соответствующими затратами. Группировка по соответствующему виду затрат приводит к информации о дебетовых и кредитовых оборотах и сальдо.

Классификация методов управленческого учета остается актуальной проблемой, при этом разделение методов управленческого учета является достаточно условным, если рассматривать методы управленческого учета через призму информационной бухгалтерской базы данных. Так, метод калькулирования по переменным затратам (direct costing) может быть использован, если присутствует поле, которое различает переменные или постоянные затраты в транзакции. Не случайно управленческий учет получил свое развитие в Великобритании, поскольку по ее ранним стандартам в отчете о прибыли должны были быть выделены прямые (переменные) затраты.

Постоянное развитие моделей бухгалтерского учета предлагает широкий диапазон возможных инструментов управленческого учета. При этом внедрение новых моделей и инструментов существенно осложняется необходимостью оценки выгоды и затрат от их внедрения.

Нами предлагается рассматривать управленческий учет, в том числе стратегический, как определенный набор методов или инструментов, степень важности которых может меняться от одной области к другой или от одного предприятия к другому, поскольку система внутреннего учета в первую очередь зависит от потребности в информации и личной точки зрения руководителей.

Каждая организация может использовать более одного инструмента управленческого учета, поэтому можно говорить о портфеле инструментов для каждой организации, сочетающем в себе как цену (затраты на внедрение и поддержание инструментов), так и качество (полезность инструментов для принятия решений). Затраты на инструменты могут быть снижены за счет выявления общности в этих инструментах, поиск которой представляет отдельный теоретический и практический интерес.

В условиях значительного государственного регулирования некоторые инструменты из статуса произвольных к использованию превращаются в обязательные, хотя такое требование может быть неявным. Понимание данного обстоятельства может способствовать развитию и внедрению соответствующих инструментов, как для информационного обеспечения принятия решений, так и для снижения рисков в системе подотчетности. Затраты на внедрение таких инструментов могут быть значительно снижены за счет выявления связи между различными инструментами и формирования общего ядра (поле в базе данных) новой информационной системы бухгалтерского учета предприятия. В конечном итоге усиление требований к подотчетности в государственном секторе экономики может приводить к снижению барьера для применимости новой системы учета, которая, в первую очередь, должна ориентироваться на цели подотчетности в условиях государственного финансирования.

Следует отметить, что помимо отнесения инструментов менеджмента к инструментам управленческого учета на основе использования в этих инструментах методов бухгалтерского учета и деления инструментов управленческого учета на операционные, управленческие и стратегические группы можно предложить деление инструментов по степени требования к их применению на обязательные, условно-обязательные и свободные.

Использование бухгалтерских информационных баз данных способствует изменению методики проведения аудита и финансового мониторинга. Аудит и финансовый мониторинг становиться похожими на Data Mining, особенно при поиске нетипичных операций. Нетипичные операции выборке из нескольких компаний формируют типологию искажений в финансовой отчетности, хищения активов и мошенничества.

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

СЕКЦИЯ 1.
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ГОСУДАРСТВЕННОМ И ЧАСТНОМ СЕКТОРАХ ЭКОНОМИКИ

СОДЕРЖАНИЕ

СЕКЦИЯ 4.
АРХИТЕКТУРА КОМПЬЮТЕРОВ И СЕТЕЙ ДЛЯ РАЗРАБОТКИ И ОСУЩЕСТВЛЕНИЯ БЕЗОПАСНЫХ СИСТЕМ

СЕКЦИЯ 5.
МЕТОДЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА И НАДЕЖНОСТИ, ОТКАЗОУСТОЙЧИВОСТИ И ЖИВУЧЕСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

СЕКЦИЯ 6.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТ-СИСТЕМАХ

СЕКЦИЯ 8.
ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР, ПОЛЬЗОВАТЕЛЕЙ, ИХ ДАННЫХ И ИНТЕРЕСОВ

СОДЕРЖАНИЕ

СЕКЦИЯ 9.
СЕТЕВАЯ БЕЗОПАСНОСТЬ

СЕКЦИЯ 10.
МЕНЕДЖМЕНТ ИННОВАЦИЙ В СФЕРЕ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

СОДЕРЖАНИЕ