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

«Проблемы информационной безопасности»

Труды III Международной научно-практической конференции

Симферополь – Гурзуф, 16-18 февраля 2017 г.

Симферополь

2017

УДК 004.056:621.391
ББК 32.972.53
П781

П781 **Проблемы информационной безопасности:** Труды III Международной научно-практической конференции, Симферополь-Гурзуф, 16-18 февраля 2017 г. — Симферополь : ИП Зуева Т.В., 2017. — 190 с.
ISBN 978-5-9908989-1-2

В сборнике размещены материалы анализа проблем информационной безопасности в решении задач планирования, разработки, внедрения, эксплуатации и развития информационных и телекоммуникационных систем, которые используются для поддержки текущей хозяйственной деятельности, стратегического планирования и процесса принятия решений в бизнесе и государственном управлении.

Также в сборнике содержатся материалы по исследованию основных проблем информационной безопасности в функционировании экономических систем управления, изучению подходов формирования новой отрасли знаний, отражающей возможность управления рисками в контексте создания системы информационной безопасности применительно к проблемам крупных корпоративных информационных систем частного сектора экономики и электронного правительства.

УДК 004.056:621.391
ББК 32.972.53

ISBN 978-5-9908989-1-2

УДК 004.8.37

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

ЗАЩИТА МЕНТАЛЬНОЙ ИНФОРМАЦИИ

Введение. Проблема информационной безопасности решается, в основном, в области технологий и связана с нарушением данных, хранящихся в компьютерных системах. Государство Российская Федерации много внимания уделяет защите персональных данных, каждый гражданин России при обращении в различные официальные организации подписывает согласие на обработку персональных данных. Несмотря на меры предосторожности, на рынке информационных услуг периодически появляются предложения о продажах различных баз данных, и практически каждый пользователь Интернет получает электронные письма от неизвестных адресатов, которым каким-то образом попал адрес пользователя без его ведома и согласия. Для защиты от спамов, кибератак и другого несанкционированного доступа к данным разрабатываются различные математические и информационные методы и технологии, имеются многочисленные научные публикации. Однако, как показал научный поиск автора, практически отсутствуют исследования по защите ментальной информации, т.е. данных, накопленных каждым индивидов в процессе обучения и собственной практической деятельности. Необходимость защиты когнитивных данных, сохранения их целостности и адекватности окружающей среде обусловили актуальность темы исследования.

Анализ публикаций по смежным вопросам выявленной проблемы показал, что пониманию и представлению смысла получаемой информации при формальном ее представлении, анализу рекламных и других текстов, отражению смысла сообщений в виде ментальных моделей, посвящено достаточное число научных публикаций, но они имеют разрозненный характер, относятся к различным областям знаний и не освещают вопросы защиты ментальной информации. Так, национальным особенностям использования Интернет посвящены работы Е.В. Бродовской и А.Ю. Домбровской; влиянию информационных потоков на сознание современного человека, особенно молодого, конструирование им социальной среды и культуры, формирование концептуальной картины мира в целом и ментальности современных поколений посвящены работы А.Б. Денисовой и В.Г. Сенюшиной, Е.А. Шишкиной, Т.Н. Сыроваткиной П.Ю. Тенхунен и Ю.А. Елисеевой, Ф.Г. Самигулиной,; проблемы семантических процессов в сознании рассмотрены в трудах М.Ю. Шульженко и В.Б. Поповской, Т.Ю. Сазоновой; к вопросам степени понимания смысла, в том числе сведений, получаемых через Интернет, относятся статьи Д.В. Полежаева, А.Г. Мухиддинова, Н.А. Седовой; достаточно большое число результатов исследований по применению ментальных (когнитивных) карт в обучении получено И.Ю. Шитовой и В.П. Гончаровой, А.И. Евтушенко и Я.Д. Фейгин и др.

Целью данной работы является определение механизмов и факторов возможной защиты ментальной информации на основе моделей ее представления и процессов формирования.

Результаты исследования. Изложим кратко выявленные аспекты проблемы и пути ее возможного решения.

Когнитивные модели представления информации в памяти человека берут свое начало в 60-х годах прошлого века, когда появилось программированное обучение, заключающееся в пошаговом формировании знаний и теория формирования действий, основанные, в свою очередь, на теориях бихевиоризма – поведении человека. В дальнейшем на основе данных подходов получили свое развитие когнитивная психология, основанная на аналогии усвоения информации человеком с работой компьютера, когнитивная экономика, как теория экономики знаний, формальные модели представления знаний для их размещения в памяти компьютера и другие. Бихевиоризм лег в основу нейроэкономики, объясняющей экономическое поведение человека в том числе, на основе рефлексов Павлова. В настоящее время данные теории стали активно использовать в обучении и других коммуникациях, в том числе межкультурных и в виртуальной среде Интернет. Главное в указанных подходах - передача и усвоение некоторого смысла, желательно, одинакового для передатчика и приемника. Здесь и возникает ряд проблем, связанных с защитой ментальной информации:

- учет национальных особенностей менталитета при восприятии нового знания и при целенаправленном его поиске в Интернет;

- формирование цельной личности в условиях «бурного и мутного» информационного потока: внутренне непротиворечивой по своим теоретическим концепциям и адекватно реагирующей на внешние воздействия;
- воспитание стратега и тактика, способного ставить дальние цели и формулировать задачи по их достижению;
- выставление когнитивных фильтров и координация семантических процессов сознания путем предоставления доступной, научной, непротиворечивой информации в различной степени детализирующей запрос пользователя;
- мозаичная структура знания при самостоятельной работе с Интернет, сложность установления связи между отдельными модулями знаний, и в связи с этим, появление ложных представлений об объектах и явлениях реального мира;
- различная степень понимания смысла некоторого понятия, наличие ментального «мусора»;
- необходимость создания целостной картины некоторой предметной области в различных формах представления (знак, текст, изображение, мелодия);
- использование когнитивных (ментальных) карт для пошаговой детализации понятий предметной области, навигации в связях между понятиями, масштабирование понятий при их взаимосвязях и детализации.

Выводы. Поставленные проблемы позволяют выработать систему защиты ментальной информации у обучающихся различных уровней образования, пользователей Интернет и исследователей, желающих выработать новое непротиворечивое и достаточно истинное знание.

УДК 004.056.01

Бойченко Олег Валериевич
д.т.н., профессор,
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

СИСТЕМА SDS NG В ЗАЩИТЕ КОММЕРЧЕСКИХ ДАННЫХ ПРЕДПРИЯТИЯ

Современное толкование понятий информационной безопасности и защищенности конфиденциальной информации во все большей степени находит свое отражение в комплексном, системном подходе к созданию адекватной, упреждающей системы защиты данных, необходимой для создания условий принятия обоснованного управленческого решения во всех сферах деятельности государства.

Подтверждением этому, стало принятие новой Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ №646 от 05.12.2016 г. В данном важнейшем нормативно-правовом акте, в частности указано на необходимость формирования новой государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию системы информационной безопасности. Это обусловлено, прежде всего, стремительным развитием информационных технологий, сетевой инфраструктуры, необходимость использования которых призвана обеспечить высокий уровень условий благоприятствования в социальном и экономическом развитии государства, общества и личности. Однако, это обусловлено также и стремительным ростом киберпреступности, отягощающей конструктивные меры по развитию личности, общества и государства не только в социально-экономическом аспекте, но и в сфере национальной безопасности государства. Так, по данным экспертов, количество выявленных ИТ-преступлений в РФ удваивается ежегодно.

В настоящее время особый статус приобретает проблема информационной безопасности в экономической сфере, что обусловлено, прежде всего, недостаточностью уровня развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Отягощающим фактором, в части отмеченного обстоятельства, является высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий, касающихся аппаратно-программных средств и средств связи, что приводит к зависимости социально-политического развитии РФ от геополитических интересов зарубежных государств.

Потому стратегическими целями о области информационной безопасности в экономической сфере являются минимизация уровня негативного воздействия

дестабилизирующих факторов, связанных с недостаточностью развития отечественной отрасли информационных технологий и средств вычислительной техники, разработка конкурентоспособных средств обеспечения информационной безопасности, а также повышение качества услуг в сфере обеспечения информационной безопасности.

Таким образом, Президентом поставлена серьезная задача по решению первоочередных вопросов совершенствования всей системы информационной безопасности государства, что влечет за собой разработку новых подходов к оптимизации функционирования действующих систем защиты, с целью их наращивания и развития, соответственно образующимся новым уязвимостям и угрозам.

На наш взгляд решение проблемы, во-первых, должно быть системным, а во во-вторых, конструктивным процессом. Потому оптимизация функционирования системы защиты данных в процессе автоматизации управления деятельностью экономического предприятия должна быть нацелена на максимально эффективное применение отработанных механизмов защиты путем их совершенствования и постепенной замены для разработки инновационной системы информационной безопасности предприятия.

Следует подчеркнуть, что сама система информационной безопасности является прикладным понятием, ее предметом является комплекс программно-аппаратных и инженерно-технических средств, функционирование которого направлено на минимизацию угроз данным, необходимым для управления и развития деятельности организации, учреждения, ведомства, министерства, государства. Данный комплекс является частью информационной системы управления, ее подсистемой, использующей в своей работе алгоритмы и приложения, являющиеся основой функционирования самой системы управления. Потому наиважнейшим вопросом совершенствования системы информационной безопасности, является совершенствование встроенных инструментальных (аппаратно-программных) механизмов защиты. При чем, на наш взгляд, основной упор необходимо сосредоточить на совершенствование механизмов защиты, ориентированных на сетевые технологии в архитектуре информационных систем управления.

Так, достаточно эффективным инструментом повышения эффективности действующей системы защиты данных в управлении экономическим предприятием может быть использование программно-аппаратного комплекса Secret Disk Server New Generation (SDS NG) для защиты корпоративных хранилищ данных, использующих платформу MS Windows Server. SDS NG является современным программно-аппаратным комплексом защиты корпоративной информации (баз данных, файловых архивов, бизнес-приложений и их данных), хранящейся и обрабатывающейся на серверах и рабочих станциях под управлением ОС Microsoft Windows.

С помощью SDS NG можно защитить от несанкционированного доступа информацию на:

- файловых серверах и архивных копиях;
- системах управления базами данных (СУБД);
- почтовых серверах;
- различных бизнес-приложениях, имеющих многоуровневую архитектуру и предоставляющих пользователям сервисы прикладного уровня (например, системы документооборота, ERP- и CRM-системы).

SDS NG использует проверенную и надежную технологию защиты данных методом их «прозрачного» шифрования, а также выполняет контроль доступа по сети к защищенным дискам.

Новой и самой интересной возможностью используемого в SDS NG механизма защиты конфиденциальной информации является опция по блокированию прямого доступа для сотрудников к корпоративным базам данных, что исключает возможность несанкционированного копирования и кражи конфиденциальной информации.

Таким образом, персонал не может работать с базами данных напрямую. Разрешен только опосредованный доступ через серверные приложения, благодаря чему неблагонадежные пользователи или даже «обидевшийся» системный администратор не могут ни выкрасть, ни модифицировать важные данные.

Применение цифровых сертификатов X.509 позволяет легко интегрировать SDS NG в корпоративную инфраструктуру, использующую открытые ключи (PKI, Public Key Infrastructure).

При этом компоненты SDS NG можно устанавливать как на один и тот же сервер, так и на различные компьютеры в любых сочетаниях, что обеспечивает условия гибкой интеграции анализируемого механизма защиты в действующую систему информационной безопасности и

создает условия для повышения уровня ее эффективности в защите коммерческих данных предприятия.

УДК 004.7.056.53

Воробьев Владимир Иванович
г.н.с., д.т.н., профессор
Евневич Елена Людвиговна
с.н.с., к.ф.-м.н.
Санкт-Петербургский институт
информатики и автоматизации Российской академии наук
Санкт-Петербург, Россия

ОНТОЛОГИЧЕСКИЕ МЕТОДЫ КОНТРОЛЯ ДОСТУПА В ОБЛАЧНОЙ СРЕДЕ

По мере развития распределенных, GRID-, «повседневных (ubiquitous), облачных (cloud), туманных (fog), росистых (dew)» и других метафорических технологий и вычислительных сред возрастают актуальность и сложность обеспечения контроля доступа к различным ресурсам и данным пользователей. При создании различных систем контроля доступа, как правило, учитывается контекстная информация пользователей – ролевой, пространственный, временной и др. контексты. В вычислительных средах, где роли пользователей и контекстная информация динамически изменяются и определяются в режиме реального времени, учет различных типов контекстной информации для обеспечения роли или изменения разрешений, безусловно, необходим для динамического контроля доступа. Модели контроля доступа бывают в основном трех типов: MAC (mandatory access control) – принудительное управление доступом; DAC (discretionary access control) – избирательное управление доступом; RBAC (role based access control) – ролевое управление доступом.

К последнему типу относятся многие современные системы (CGRBAC, ARBAC97, SRBAC, X-GTRBAC, SCARBAC, GEO-RBAC, SG-RBAC), учитывающие ролевой контекст пользователя, в которых права доступа предоставляются роли пользователя. Их широкое применение обусловлено их большей гибкостью. Роли пользователей изменяются динамически вместе с изменением контекста. Но не все эти системы подходят для управления доступом, например, в облачной среде, так как ARBAC97, CAB-RBAC и S-RBAC не учитывают ни временного, ни пространственного контекстов, ни доверительного уровня платформы; GTRBAC и X-GTRBAC тоже недостаточно гибки в отношении пространственных ограничений; SCA-RBAC, GEO-RBAC, SG-RBAC и ABAC не учитывают доверительного уровня платформы.

Предлагается подход к контролю доступа к облачным ресурсам на основе рекомендующей системы, описывающей отношения элементов двух множеств: множества пользователей и множества облачных сервисов. Профиль пользователя формируется на основе метаданных пользовательских запросов, анализа содержания запросов и статистики действий. В процессе оценки прав доступа пользователя учитываются: детали запроса, анализ его содержания, частота доступа и другие статистики действий пользователя, например, полнота и время просмотра результатов, правки, комментирование. Метаданные характеризуют тип запроса и его содержание, предметные области интересов пользователя, часто используемые пользователем термины, ключевые слова. Предлагается также использовать статистику запросов к различным ресурсам по их типу: открытые материалы; защищенные материалы; административные материалы; индексация каталога.

Профиль пользователя строится в поэтапно: сбор, анализ информации и построение онтологии предметной области интересов. Для построения онтологии используются среды разработки и анализа онтологий. Они обеспечивают интерфейсы, которые позволяют выполнить концептуализацию, реализацию, проверку непротиворечивости и документирование, поддержку документирования онтологий, импорт и экспорт онтологий разных форматов и языков, поддержку графического редактирования, управление библиотеками онтологий, etc.

Кроме того, средства онтоинженерии позволяют сопоставлять построенную онтологию профиля пользователя с онтологиями библиотеки профилей злонамеренных пользователей и блокировать доступ в случае совпадения.

По прогнозам компании Cisco в достаточно близкой перспективе (за период 2015-2020 г.г.) количество подключенных к Internet устройств и объектов увеличится примерно в 2 раза – с 25 до 50 миллиардов. Интернет вещей, повсеместные, туманные, росистые и прочие «пасмурные и дымчатые» вычисления – все вышесказанное приведет к возрастанию динамики изменений, в

частности, различных контекстов в отношении резко возрастающего числа объектов. Представляется возможной ситуация стирания граней между пользователем и ресурсом – в каком-то смысле объектами будущих в высокой степени «рассеянных» сред будут пользователи и они же ресурсы одновременно. Предложенный онтологический подход представляется перспективным с точки зрения быстроты реагирования на происходящие изменения и развитие ситуации.

УДК 004.6

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

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В нынешних условиях функционирования бизнеса информация приобрела особую роль, став на один уровень с продажей товара или реализацией услуги. Поэтому продажа или покупка информации стали обыденным явлением современной действительности, что, бесспорно, имеет свои преимущества. В качестве доказательств о существовании этих преимуществ приведем некоторые аргументы:

- информация – конечный результат маркетинговых исследований;
- информация – оформляется в виде официальных документов;
- информация – основа для принятия управленческого решения;
- информация – основа для планирования;
- информация – инструмент конкурентной борьбы;
- информация предупреждает, повышает осведомленность, придает уверенности.

Но наряду, с уже перечисленными преимуществами, существуют и негативные моменты, связанные с использованием информации. Так, по своему характеру информация может быть секретной, а значит, всегда будет повод для несанкционированного доступа к ней. Даже этот аспект уже указывает на существующую и постоянную угрозу для предприятия. Источников или причин возникновения таких угроз, связанных с информацией, не мало, поэтому актуальна проблема обеспечения информационной безопасности предприятия.

С теоретической точки зрения, обеспечение информационной безопасности – это совокупность мероприятий, направленных на соблюдение конфиденциальности, целостности и доступности информации. Исходя из сказанного, информационная безопасность характеризуется определенным состоянием информационного объекта и деятельностью предприятия по защите этого объекта. Эти характеристики, по нашему мнению, можно отождествлять с критериями эффективности обеспечения информационной безопасности предприятия. Рассмотрим их более подробно.

Под информационным объектом может выступать информация в виде сведений, данных, ведомостей, цифр и др. Также в качестве информационного объекта может быть информационный ресурс, поданный как информационная система предприятия или автоматизированная система предприятия. В свою, очередь, к каждому из указанных информационных объектов предъявляются определенные требования, что позволяет оценить их состояние.

Усилия предприятия по защите информационного объекта должны быть направлены на:

- регламентирование деятельности предприятия при помощи нормативно-правовых документов, связанных с информационной защитой и разработанных на федеральном, региональном и местном уровнях;
- генерирование внутренней нормативной документации (приказов, положений, инструкций, распоряжений, концепций, стратегий и др.), которые разработаны предприятием для своих нужд, и также, связанных с обеспечением информационной безопасности;
- создание структурного подразделения, занимающегося обеспечением информационной безопасности предприятия или, если речь идет о небольших предприятиях, - выделение в штатном расписании должности специалиста по обеспечению информационной безопасности;

- формирование четкого перечня требований, задач, должностных инструкций, выдвигаемых к структурным подразделениям и специалистам, обеспечивающим информационную безопасность предприятия;
- приобретение предприятием технических средств, программных продуктов, обеспечивающих его информационную безопасность, и периодическое обновление программно-технического парка;
- оборудование и обеспечение защиты специальных помещений, где осуществляется обработка и хранение информации в документальной форме на бумажных носителях (архивы);
- выбор специалистами предприятия методов, способов, инструментов и приемов обеспечения информационной безопасности;
- разработка внутренних правил получения, хранения, накопления и передачи информации, представляющей коммерческую и иную ценность для предприятия;
- группировку информации по разным признакам и определение круга пользователей для каждой из групп;
- оформление журналов регистрации информационных потоков, как на электронных, так и на бумажных носителях;
- определение четких процедур и случаев доступа к разным группам информации о предприятии.

Определенную угрозу для предприятия могут составлять и манипуляции с информацией, которые осуществляются, как во внутренней среде предприятия, так и во внешней. К таким манипуляциям отнесем разглашение, раскрытие, сокрытие, искажение, изменение, уничтожение, блокирование информации.

Таким образом, основными задачами по обеспечению информационной безопасности предприятия являются создание соответствующей эффективной системы, выработка политики и механизма.

Система управления информационной безопасности предприятия объединяет в себе субъектов (разработчики и пользователи информации) и объектов (информационные ресурсы, информационные системы). Политика обеспечения информационной безопасности отображает формальные аспекты формирования и использования информации, заключенные в директивах, инструкциях, регламентах и др. Механизм обеспечения информационной безопасности представлен инструментами, методами и способами, предназначенными для рационального генерирования и использования конфиденциальной и иной информации.

Характеризуя механизм обеспечения информационной безопасности предприятия, акцентируем внимание на таких его составляющих, как контроль доступа к информации, аудит и мониторинг информации, идентификация, аутентификация и авторизация участников информационных потоков, обеспечение пользователям информации благоприятных условий работы, варианты реакций на случаи нарушения информационной безопасности, варианты реакций на случаи подозрений относительно нарушения информационной безопасности. Немаловажной составляющей механизма обеспечения информационной безопасности предприятия является такое действие со стороны его персонала как поддержание работоспособности информационной среды, гарантирующей эффективный, быстрый, а самое главное, безопасный обмен информацией между пользователями.

Резюмируя сказанное, отметим, что обеспечение информационной безопасности, а также управление информационной безопасностью предприятия, основываются на системном и процессном подходах. Это дает более широкие возможности для выбора вариантов в соответствии с целями субъекта защиты.

УДК 004.056.5

Дмитриев Владимир Александрович
заведующий лабораторией, к.ф.-м.н.
Степанян Арарат Баркевович
ведущий научный сотрудник, к.т.н.
Афанасьев Александр Владимирович
ведущий инженер-программист
Объединенный институт проблем информатики
Национальной академии наук Беларуси, Республика Беларусь

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

ИТ-инфраструктура современного предприятия отличается высокой сложностью и разнообразием. Используемые системы защиты постоянно развиваются и адаптируются к новым видам угроз. При этом число источников, из которых поступают информация по текущему состоянию защищенности, непрерывно растет. Администраторам информационной безопасности все сложнее следить за общей картиной происходящего. А ведь если своевременно не анализировать возникающие угрозы и не пытаться предотвратить их, любая система защиты информации окажется бесполезной. Проведение анализа защищенности позволяет заблаговременно выявить наиболее уязвимые компоненты корпоративных информационных сетей (КИС) и устранить недостатки в обеспечении защиты.

Поэтому крайне актуальной задачей является разработка систем мониторинга, анализа и корреляции событий информационной безопасности КИС, которые позволят отслеживать не только текущее состояние КИС с точки зрения информационной безопасности, но и изменения в ней как в динамической системе, т.е. проводить анализ защищенности. К таким системам относятся SIEM системы. Данные системы позволяют автоматизировать процесс анализа событий поступающих от различных устройств КИС и повысить эффективность управления сетевой инфраструктурой в целом, таким образом, упрощая задачу защиты информации.

В Объединенном институте проблем информатики Национальной академии наук Беларуси разработана SIEM-система – программный комплекс системы мониторинга состояния информационной безопасности (ПК СМСИБ).

ПК СМСИБ представляет собой набор программных модулей, которые объединены в систему для контроля состояния ИБ с целью организации и улучшения обнаружения и отображения событий безопасности.

Назначение ПК СМСИБ:

− оперативное обнаружение атак и нарушений политики информационной безопасности;

− соотнесение в режиме реального времени событий от разных устройств, выявление инцидентов ИБ и их приоритезация;

− автоматическое реагирование на инциденты;

− формирование базы знаний по инцидентам;

− проведение аудитов и расследований инцидентов;

− оценка уровня угроз для отдельных корпоративных ресурсов.

Состав ПК СМСИБ:

− сервер приложений;

− база данных;

− консоль управления;

− система обнаружения вторжений;

− агенты мониторинга.

Источниками событий для ПК СМСИБ являются объекты ИТ- инфраструктуры, в состав которых могут входить:

− серверы и рабочие станции под управлением ОС GNU/Linux;

− серверы и рабочие станции под управлением ОС Windows;

− базы данных журнала действий администраторов и пользователей;

− активное сетевое оборудование;

− средства защиты;

− средства мониторинга состояния антивирусной безопасности ИТ-инфраструктуры;

− средства мониторинга, контроля доступа и защиты от несанкционированного доступа к ИТ-инфраструктуре;

− средство мониторинга, контроля доступа к базае данных (MySQLProxy).

Фиксация событий информационной безопасности на объектах ИТ-инфраструктуры производится в журналах событий конечных устройств и систем, откуда с помощью агентов мониторинга данные передаются серверу приложений ПК СМСИБ.

Данные о событиях информационной безопасности, полученные от соответствующих агентов, передаются на дальнейшую обработку в модуль корреляции после записи данных в базу данных ПК СМСИБ.

Модуль корреляции сервера приложений выполняет автоматический анализ собранных данных и обеспечивает выявление инцидентов информационной безопасности с помощью набора правил корреляции для сравнения зарегистрированных событий информационной безопасности (записей журналов регистрации) с шаблонами известных сетевых угроз безопасности.

ПК СМСИБ обеспечивает:

− автоматический анализ и обнаружение компьютерных атак (вторжений) на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным;

− отображение обнаруженных атак (вторжений) в веб-интерфейсе консоли управления ПК СМСИБ и уведомление администратора безопасности об обнаруженных атаках по электронной почте;

− автоматическое сохранение истории обнаруженных событий и атак (вторжений) для последующего анализа;

− поиск событий и атак (вторжений) в соответствии с заданными правилами;

− экспорт журнала атак (вторжений) в файл для последующего импорта в сторонние приложения;

− обновление баз правил обнаружения атак (вторжений);

− выборочное использование отдельных правил обнаружения или группы правил;

− добавление собственных правил для анализа сетевого трафика;

− отображение и экспорт в файл формата PCAP IP-пакеты, соответствующие зарегистрированным атакам (вторжениям);

− контроль целостности исполняемых файлов;

− контроль целостности загружаемых баз правил обнаружения атак.

УДК 33.338.2

Мандрица Игорь Владимирович
д.э.н., профессор кафедры ОТЗИ ИИТТ СКФУ
Мандрица О. В.
к.э.н., доцент, кафедры ЭАиА ИЭУ СКФУ
Соловьева И. В.
к.э.н., доцент, кафедры ЭАиА ИЭУ СКФУ
Петренко В. И.,
к.т.н., доцент кафедры ОТЗИ ИИТТ СКФУ
Ставрополь, Россия

БЮДЖЕТОЗАЩИЩЕННОСТЬ КАК ПОКАЗАТЕЛЬ ТЕХНИКО-ЭКОНОМИЧЕСКОГО ОБОСНОВАНИЯ ПРИНИМАЕМЫХ РЕШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЮДЖЕТНЫХ ОРГАНИЗАЦИЙ

Защита информации в бюджетной сфере достаточно специфический и важный вид деятельности для всех агентов хозяйственного механизма страны. Бюджетные организации тратятся на создание собственных условных информационных единиц для последующего оказания ими государственных услуг. Специфика информационной защиты бюджетных организаций заключается в том, что чтобы защитить создаваемые ими условные информационные единицы, в процессе оказания и предоставления ими государственных услуг. Бюджетные организации подвержены тем же рискам потери информации, что и все агенты рынка. В вопросе оправданности основных и дополнительных трат на защиту информации существует единая концепция – траты на защиту информации всегда направлены на уменьшения возможного риска ее потери и ущерба.

Одним из показателей подтверждающих оправданность таковых трат является показатель - Бюджетозащищенность. Новейшие теоретические исследования в данном направлении по

изучению подходов и разработки основ бюджетозащищенности были рассмотрены ранее в работах вышеназванных авторов.

Бюджетная организация с помощью навыков и компетенций развивает свой вид деятельности, создает условные информационные единицы (базы данных, персональные данные), в процессе оказания и предоставления ими государственных услуг и хочет быть уверена, в том, что ее деятельность является безопасной для реализации ее конечной цели – бесперебойное и качественное предоставление государственной слуги. Возникает вопрос – каковы должны быть затраты (издержки) на создание такого рода информационной защиты, чтобы экономически это было соразмерно, или, как говорят экономисты – обосновано.

Нельзя допустить, чтобы затраты на защиту информации превышали саму стоимость государственной услуги, или другими словами – стоимость защиты не превышала бы величину ущерба от потери информации в процессе оказания государственной услуги.

Защита информации субъектов государства необходима, но должна быть обоснована и не превышать суммы возможных ущербов. В этой связи и потребовалась разработка эффективного подхода (метода) по обоснованию необходимых сумм затрат на информационную безопасность бюджетных единиц.

Ведь квинтэссенцией всей обоснованности выступает бездефицитность бюджета страны, а именно его факторы в части расходов на его статьи и полученных доходов государства в виде налогов, пошлин и прочих поступлений.

Для понимания глубины и широты данной задачи актуальным становится теоретический аспект – разработка механизма обоснования затрат на информационную безопасность субъектов государства, а именно ее бюджетных организаций.

Рассмотрим новый теоретический подход (метод) обоснования мероприятия по повышению ИБ бюджетной организации на примере любой бюджетной организации, например в рамках защиты ее персональных данных (далее ПДн). Основным показателем – критерием выбора наиболее рационального мероприятия по повышению информационной безопасности будет рост показателя бюджетозащищенности образовательного учреждения ДО и ПОСЛЕ мероприятий по защите информации.

Рассчитаем текущее значение показателя бюджетозащищенности для бюджетной организации ДО мероприятия повышения защищенности ПДн, согласно формуле бюджетозащищенности (1):

$$\Delta BSU_{2016} = \frac{\left(R_{Afterevents} - R_{Beforeevents}\right) \cdot \left(B_{2016} - \sum Events_{BSU}\right)}{B_{2016}} \quad (1)$$

Где ΔBSU_{2016} - изменение бюджетозащищенности ПДн за период;

B_{2016} - бюджет за период 2016 год, рублей;

$\sum Events_{BSU}$ - сумма на решение по повышению защиты ПДн увеличивающее бюджет за период 2016 год, рублей;

$\left(R_{Afterevents}\right)$ - вероятность угрозы ущерба ПОСЛЕ решения, отн. число;

$\left(R_{Beforeevents}\right)$ - вероятность угрозы ущерба ДО решения, отн. число;

Где сама вероятность ущерба рассчитывается по формуле 2:

$$R = \rho\, BSU * C\, BSU \quad (2)$$

Где ρ BSU - вероятность угрозы ущерба для бюджета, отн. число,
C BSU - сумма угрозы ущерба для бюджета от потери или утечки ПДн информации, рубли.

Обоснованием рациональности предлагаемого решения повышения информационной безопасности будет рост показателя бюджетозащищенности ПОСЛЕ мероприятия. То есть, показатель бюджетозащищеность ПДн должен опережать предыдущие значения защищенности по формуле (3 и 4):

$$BSU_{2016} > BSU_{2015} \quad (3)$$

Где

$$BSU_{2015} = \frac{\rho\, BSU * C\, BSU * \left(B_{2015}\right)}{B_{2015}} \quad (4)$$

Расчет рисков по угрозе информационной безопасности бюджетной организации необходимо производить по каналам угроз ПДн. При работе с алгоритмом используется шкала

от 0 до 100%. Максимальное число уровней – 100, т.е. шкалу можно разбить на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта разделения: равномерное и логарифмическое. Вначале рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость.

Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации (5).

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100} \times \left(1 - \frac{s}{100}\right), \quad (5)$$

где ERc,I,a – критичность реализации угрозы (указывается в %);
P(V)c,I,a – вероятность реализации угрозы через данную уязвимость (указывается в %),
S – степень сопротивляемости контрмеры (%), определяется экспертными оценками.

Таким образом, получив расчеты РОСТА показателя бюджетозащищенности для бюджетной организации (на примере защиты ее ПДн) ДО и ПОСЛЕ мероприятия, мы получаем достаточно обоснованный критерий принятия или отклонения предлагаемого мероприятия повышения информационной безопасности ПДн

УДК 330.332

Павлов Константин Викторович
д.э.н., профессор
ЧОУ ВО «Камский институт гуманитарных и инженерных технологий»
г. Ижевск, Россия

УПРАВЛЕНИЕ ЭКОНОМИКОЙ С УЧЕТОМ ОЦЕНКИ ВОСПРОИЗВОДСТВЕННЫХ ДИСПРОПОРЦИЙ

В связи с тем, что в настоящее время сложность производственных процессов неизмеримо возросла, чрезвычайно усложнилась и проблема поиска методов эффективного управления и обеспечения устойчивого функционирования экономикой. В условиях переходного периода, когда существенно возросли нестабильность и изменчивость организационно-экономической среды, вопросы управления и социально-экономического прогнозирования естественным образом выдвигаются на первый план. Одной из важнейших причин возросшей в последнее время неопределенности и изменчивости социально-экономической среды является углубление различного рода воспроизводственных диспропорций. Учитывая все сказанное, целесообразно, на наш взгляд, рассмотреть некоторые направления управления и хозяйствования при переходе к рынку, в условиях высокого уровня изменчивости экономической среды. Так, ряд исследователей выделяет несколько этапов в развитии систем общефирменного управления за рубежом. К таким этапам относятся управление на основе контроля за исполнением, управление на основе экстраполяции, управление на основе предвидения изменений и управление на основе гибких экстренных решений, которое складывается в настоящее время, в условиях, когда многие трудности возникают настолько неожиданно, что их невозможно предусмотреть.

Усложнение производственных процессов и рост нестабильности организационно-экономической среды приводят к необходимости разработки решения уже тогда, когда из внешней среды поступают сравнительно слабые сигналы. В связи с этим в новых условиях хозяйствования неизмеримо возрастают роль и значение планирования и прогнозирования, но не того типа планирования, которое действовало в условиях социалистического способа производства. Присущие ему свойства инерционности, переноса на перспективу существующих тенденций и условий хозяйствования и т. п. не только делают невозможным применение этой формы планирования в полном объеме в настоящее время, но и являются одной из важнейших причин низкой эффективности социалистической экономики. В связи с необходимостью приспособить существующую систему управления к качественно новым условиям, сделать ее гибче и лабильнее, в развитых капиталистических странах используется несколько форм планирования. В системе долгосрочного планирования предполагается, что будущее может быть предсказано путем экстраполяции исторически сложившихся тенденций роста. В системе же стратегического планирования не считается, что будущее можно изучить методом экстраполяции. Здесь вначале предпринимается анализ перспектив фирмы, в ходе которого исследуются тенденции, шансы фирмы, а также отдельные чрезвычайные ситуации, которые способны изменить сложившиеся тенденции. Следующим этапом является изучение позиций в

конкурентной борьбе. На этапе, получившем наименование метода выбора стратегии, осуществляется сравнение перспектив фирмы в различных видах деятельности, происходит установление приоритетов и распределение ресурсов между различными видами деятельности для обеспечения будущей стратегии.

Таким образом, под стратегическим планированием понимается управленческий процесс создания и поддержания стратегического соответствия между целями фирмы, ее потенциальными возможностями и шансами в сфере рынка. Далее разрабатываются детализированные планы отдельных видов производств и выпуска конкретных товаров и марочных изделий, что в целом обозначается как планирование маркетинга. Различают еще тактическое, оперативное и т. п. формы управления и планирования. Наличие различных форм, видов и методов планирования и управления, на наш взгляд, являет собой наглядный пример попытки приспособиться к неопределенности экономической среды, к росту сложности и нестабильности социальных процессов.

Переход на рыночные отношения российской экономики, многочисленные ошибки, возникшие вследствие непродуманности и отсутствия цельной, глубокоразработанной, логичной концепции этого перехода также приводят к росту нестабильности организационно-экономической среды. Все это, с одной стороны, делает невозможным использование той жесткоцентрализованной, директивной формы планирования и управления производством, которое было характерно для социалистического периода развития, с другой стороны, крайне актуализирует поиск новых форм и методов управления и планирования, ибо, как доказывает мировой опыт, без использования определенных вариантов осуществления управленческих процессов современное производство просто невозможно. В этой связи для российских предприятий в настоящее время в целях повышения эффективности их производственной деятельности целесообразно использовать некоторые элементы, характерные для системы управления западными фирмами.

Прежде всего, на наш взгляд, следует отказаться от попытки осуществить всеобъемлющее планирование всех сторон производственной и социальной деятельности коллектива предприятия и сконцентрироваться на решении важнейших проблем. В этой связи заметим, что для того, чтобы справиться и овладеть быстроменяющейся обстановкой на рынке, в развитых капиталистических странах в системе управления фирмами взят на вооружение принцип своевременных решений. Данный подход весьма эффективен, а потому его использование как основы построения системы управления российскими предприятиями в современных условиях представляется своевременным и необходимым.

УДК 004.055

Пенькова Инесса Вячеславовна
д.э.н., профессор
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»,
Республика Крым, Россия

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Каждая соцсеть предполагает предоставление пользователем ей сведений при регистрации. В основном люди указывают реальные сведения о себе, и при этом вносят в информационную систему персональные данные, перечень которых довольно обширный: от ФИО до некоторых предпочтений пользователя.

В связи с тем, что любая соцсеть обрабатывает персональные данные пользователей, у менеджмента таких организаций, а в первую очередь и самих пользователей появляется потребность в повышении уровня защищенности личных данных. В этом контексте одной из приоритетных задач безопасности на данный момент можно считать обеспечение конфиденциальности, что подразумевает предоставление личных данных, в рамках соцсети, только определенному заранее кругу лиц. Помимо конфиденциальности, еще одним важным фактором является обеспечение целостности личной информации, и механизмов, отвечающих за гарантированную подлинность пользовательской страницы. Последнее требование обрело свою по причине существования страниц-клонов, с которых, как правило, производят действия недобросовестного характера злоумышленники.

Как выяснилось в ходе исследования, многие пользователи изначально планируют предоставлять меньше доступа к объему сведений о себе, чем в итоге запрашивает система.

Например, при заполнении анкеты на получение бонус-карты торговой сети, пользователю предлагают указать значительный объем личной информации. В таких случаях, желательно не указывать в анкете, к примеру, адрес проживания, потому что, для аналитики географии покупателей магазину и, тем более, социальной сети достаточно знать страну, город проживания. Сообщая о себе излишние подробностей, пользователь становится уязвимее. Располагая достаточным количеством информации о человеке, мошенники могут, выдавая себя за другого пользователя, нанести ущерб.

Возможность настраивать пользовательский доступ в соцсетях не решает проблему кардинально, так как существуют иные многообразные пути утечки данных. Часто данные, находящиеся в общем доступе, которые пользователи размещают в социальных сетях, обрабатываются сторонними сервисами. Физическое лицо всегда имеет право на изъятие своих данных путем направления соответствующего требования, по которому оператор обязан в срочном порядке прекратить обработку персональных данных лица.

На сайте каждой социальной сети размещена информация о применяемой политике конфиденциальности, т.к. по закону они обязаны осуществлять обработку ПДН пользователей в соответствии с 152-ФЗ «О персональных данных» от 27 июля 2006 г.

Защиту пользователей в сети осуществляет Роскомнадзор, проводя надзор и госконтроль за исполнением одобренных законодательных актов в сфере защиты личных данных и информации. Деятельность ведомства регламентирована: Конституцией РФ (от 12.12.1993), 152-ФЗ «О персональных данных» (от 27.07.2006), 149-ФЗ «Об информации, информационных технологиях и защите информации» (от 27.07.2006), 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (19.12.2005) и ряд других законодательных актов.

По мнению специалистов, ряд правил, входящих в ФЗ-152 выставляет интернет-коммерцию незаконной деятельностью, в это число входят и социальные сети, то есть, реализация технических средств, используемых для обработки персональных данных клиентов социальной сети. Чаще всего юридическими методами разрешаются последствия каких-либо действий. Примером может служить требование пользователя персональных данных об удалении его личных данных с Интернет-ресурса или отправка заявления об отказе на обработку личных данных. Нивелирование этих последствий следует обеспечивать комплексом программно-аппаратных решений по обеспечению защиты пользователей.

Отметим, что, несмотря на то, что специалисты расходятся во мнениях, и многие из них считают, что закон не соответствует современным тенденциям, каждый пользователь несет персональную ответственность и должен самостоятельно контролировать объем и содержание излагаемой личной информации.

УДК 044.056.04

Сизерон Мари
преподаватель
Университет София-Антиполис
Ницца, Франция

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ

Утечка конфиденциальной информации и клиентских данных – это проблема, с которой всё чаще сталкиваются компании, недостаточно ответственно подходящие к вопросам информационной безопасности.

Только за последние три года объем персональных данных и прочей конфиденциальной информации в интернете вырос на 40%.

Одновременно участились случаи преступлений, связанных с кражей персональной информации: 46% пользователей интернета сталкивались с попытками онлайн-мошенничества, а 18% крупных компаний хотя бы раз подвергались попыткам взлома своих сайтов или иным атакам интернет-преступников. Десять лет назад подобные случаи были единичными.

Растущий уровень кибер-преступлений вынуждает компании, работающие с конфиденциальной информацией, лучше защищать собственные информационные системы и данные своих клиентов.

По мнению аналитиков Teleperformance, утечка персональных данных приводит к тому, что почти две трети клиентов компании (62%) прекращают доверять ей в дальнейшем.

По мнению большинства опрошенных (65%), риск утечки персональных данных возрастает во время праздников и отпусков, когда традиционно совершается большое количество финансовых и других клиентских операций, а ответственный за информационную безопасность персонал может оказаться недостаточно бдительным.

При этом только 40% считают, что их работодатель серьезно подходит к вопросам защиты данных своих сотрудников и клиентов.

Утечка персональных данных является весьма насущной проблемой и для самих потребителей: 33% опрошенных лично сталкивались с кражей информации.

Результат подобных происшествий – недоверие к компании-виновнику утечек.

Для предотвращения подобных инцидентов, в настоящее время наиболее целесообразным является применение наиболее эффективных методов и средств защиты информации.

В первую очередь, это касается обучения сотрудников компании правилам безопасной работы с конфиденциальной информацией, в том числе с персональными данными клиентов.

При этом, особое внимание уделяется правилам работы в сети интернет и правилам общения в социальных сетях. Обучение сотрудников – важная составляющая безопасности.

По крайней мере, любой сотрудник должен знать, что нельзя открывать непонятные вложения в электронную почту, передавать собственные пароли коллегам, отключать антивирусные программы и использовать простые пароли.

Особое внимание уделяется мониторингу сетевой активности сотрудников, как части мероприятий по обеспечению информационной безопасности компании.

Следить за деятельностью сотрудников лучше всего изнутри компании. Однако, настраивать системы, которые будут собирать данные о посещаемых сотрудниками сайтах и запрашиваемых документах вполне может и внешняя компания.

Действенным способом обеспечения информационной безопасности клиентов является настройка межсетевого экрана и развертывание антивирусного решения, являющегося базовым проектом, с которого начинается создание системы защиты ИТ-среды компании.

Кроме того, подобные решения могут быть дополнены системами обнаружения внешних вторжений, а также продуктами обеспечивающими защиту ресурсов компании от внешних атак (DDoS и т.п.).

Разграничение доступа к ресурсам в корпоративной сети обеспечивает выявление **у**гроз безопасности, которые часто возникают там, где сотрудники имеют доступ к данным, часто не нужных для работы.

В том числе к документам, содержащим коммерческую тайну компании. Кроме того, ИТ-компании могут предложить разработку и внедрение корпоративных политик безопасности, систем авторизации и аутентификации, создание работающих служб управления правами пользователей.

Безопасность ИТ-систем во многом зависит от своевременной установки обновлений ПО.

Однако, с одной стороны массовая установка обновлений пользователями – большой трафик в корпоративной сети, да и не все обновления совместимы с корпоративным ПО.

Хорошей практикой является использование систем централизованной установки обновлений и разработка политик блокирующих доступ компьютеров без необходимого набора обновлений системного и антивирусного ПО в корпоративную сеть.

Угрозы безопасности компании происходят из самых разных источников. Бывают ситуации, когда компаниях теряет собственные компьютеры и все содержащиеся на них данные. При этом необходимо предотвратить доступ к данным посторонних лиц и восстановить данные на новых компьютерах. Тут поможет как разработка системы резервного копирования так и использование систем шифрования и виртуальных сред.

Организация процессов информационной безопасности – востребованная бизнес услуга.

Полноценную службу безопасности могут позволить себе только относительно крупные компании. В малом и среднем бизнесе внимание к безопасности ИТ-среды значительно меньше.

Однако, контроль за работой систем безопасности, руководство компании все же обычно оставляет себе. Впрочем, с внешним провайдером сложнее договориться о том, чтобы он «закрыл глаза» на нарушение корпоративных политик безопасности. Так что передача таких ИТ-процессов на аутсорсинг вполне способна увеличить безопасность компании.

УДК 004.056.5

Степанян Арарат Баркевович
вед.н.сотр., к.т.н.
Дмитриев Владимир Александрович
зав.лаб., к.ф.-м.н.
Максимович Елена Павловна
вед.н.сотр., к.ф.-м.н.
Объединенный институт проблем информатики
Национальной академии наук Беларуси,Республика Беларусь

ПРОБЛЕМА АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ В РЕСПУБЛИКИ БЕЛАРУСЬ

Доклад посвящен анализу систем защиты информации информационных систем и выявлению основных направлений их дальнейшего развития и совершенствования с целью удовлетворения всех необходимых требований действующего законодательства Республики Беларусь (РБ) в области защиты информации и последующей аттестации.

Проблема аттестации анализируется на примере Национальной Грид-сети РБ. Национальная Грид-сеть РБ предназначена для решения сложных задач, которые связаны с выполнением ресурсоемких расчетов или обработкой больших объемов данных и не допускают эффективного решения в рамках традиционных информационных технологий. К таким задачам относятся, например, задачи моделирования промышленных изделий и процессов, управления сложными технологическими процессами в авиа- и автомобилестроении, атомной промышленности, ракетно-космической отрасли, задачи криптографии, медицинской диагностики, разработки новых лекарственных средств, имитационного моделирования биологических процессов, управления чрезвычайными ситуациями и многие другие.

В качестве основной платформы для построения Национальной Грид-сети РБ выбрано программное обеспечение UNICORE, представляющее собой набор веб-сервисов и технологий для организации высокопроизводительной вычислительной сети. В качестве средства криптографической защиты информации (СКЗИ) используется OpenSSL – криптографический пакет с открытым исходным кодом для работы с SSL/TLS.

OpenSSL, используемый в UNICORE, поддерживает разные алгоритмы шифрования и хеширования, в том числе:

1) Симметричное шифрование – Blowfish, Camellia, DES, RC2, RC4, RC5, IDEA, AES, ГОСТ 28147-89;
2) Хеш-функции – MD5, MD2, SHA, MDC-2, ГОСТ Р 34.11-94;
3) Асимметричное шифрование и электронную цифровую подпись – RSA, DSA, Diffie-Hellman key exchange, ГОСТ Р 34.10-2001 (34.10-94).

Необходимо отметить, что ни один из перечисленных алгоритмов не сертифицирован в РБ. В то же время в статье 28 закона РБ «Об информации, информатизации и защите информации», определено, что информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь. В данной статье, также отмечается, что для создания системы защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь. Перечень всех сертифицированных в РБ криптографических алгоритмов приведен в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации». В данном приказе установлен и порядок криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам в Республики Беларусь. В данном приказе отмечается, что криптографическая защита служебной информации ограниченного распространения должна осуществляться на отдельно выделенном средстве вычислительной техники, не подключенном к информационным сетям, сетям электросвязи общего пользования, в том числе к глобальной компьютерной сети Интернет. В случае, когда такое подключение требуется для обеспечения технологических процессов

функционирования информационной системы, оно должно осуществляться с применением СКЗИ, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия РБ.

В данном приказе приведен перечень технических нормативных правовых актов и документов, в которых определены требования к криптографическим механизмам. В частности, для криптографического механизма «шифрование» в этот перечень включены: ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» и СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»; для механизма «имитозащита» – ГОСТ 28147-89 и СТБ 34.101.31-2011; для электронной цифровой подписи – СТБ 1176.1-99 и СТБ 34.101.47-2012.

Таким образом, в настоящем состоянии Национальная Грид-сеть РБ, основанная на применении OpenSSL, не соответствует действующим законам РБ, и ее невозможно аттестовать в РБ. Для аттестации Грид-сети РБ необходимо применение СКЗИ, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия РБ.

В соответствии с требованиями регулятора, в качества СКЗИ можно использовать «Программный комплекс «Сервер TLS АВЕСТ» (ПК AvTLSrv), реализующий защиту на транспортном уровне, или «Шлюз безопасности Bel VPN Gate» и «Клиент безопасности Bel VPN Client 3.0.1», реализующие защиту на межсетевом уровне, которые имеют сертификат соответствия, выданный в Национальной системе подтверждения соответствия РБ.

Программный комплекс AvTLSrv предназначен для функционирования на стороне веб-сервера и обеспечивает:

– конфиденциальность передаваемых данных;
– целостность передаваемых данных;
– взаимную аутентификацию сторон с использованием сертификата открытого ключа (СОК);
– одностороннюю аутентификацию сервера с использованием СОК.

Шлюз безопасности Bel VPN Gate обеспечивает:

– защиту транзитного трафика между различными узлами сети;
– защиту трафика самого шлюза безопасности;
– пакетную фильтрацию трафика.

Программно-аппаратное устройство Bel VPN Client обеспечивает защиту трафика между удаленным компьютером и шлюзом безопасности Bel VPN Gate. Клиент также обеспечивает пакетную фильтрацию трафика.

Таким образом, применение в UNICORE одного из указанных СКЗИ даст возможность аттестовать систему защиты информации Национальной Грид-сети РБ.

УДК 004.01

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

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ – РЕТРОСПЕКТИВА И ПЕРСПЕКТИВА

В конце минувшего 2016 года была введена в действие новая «Доктрина информационной безопасности Российской Федерации», концептуальный документ, призванный определять стратегию государства в области обеспечения информационной безопасности (ИБ) в современном понимании этого термина. Тем самым закончился довольно длительный, учитывая темпы развития информационно-коммуникационных технологий (ИКТ), период действия первой её версии 2000 года.

За прошедшие годы существенно расширились или возникли новые сферы применения ИКТ, и не будет сильным преувеличением считать, что мы уже живём в информационном обществе, в некотором смысле этого слова, поскольку практически все сферы жизнедеятельности на индивидуальном, общественном, производственном, государственном и международном уровнях стало трудно представить без их использования. Более того, на всех

уровнях фактически возникла критическая зависимость от них, что естественно внесло изменения в проблематику информационной безопасности, особенно, в индивидуальной и публичной сферах, имеющих, тем не менее, государственную важность.

Не лишним будет заметить, что Российская Федерация, приняв «Доктрину ИБ», при всех её недостатках, действительных или мнимых, стала первым государством, где на самом высоком уровне был утверждён столь масштабный интегрирующий документ, определяющий политику обеспечения информационной безопасности во всех её аспектах. А на международном уровне именно по инициативе России ещё в 1993 году при участии СПИИРАН был разработан и подготовлен для рассмотрения в ООН проект «Конвенции о запрещении военного или любого иного враждебного использования методов и средств воздействия на инфосферу» (Convention on the prohibition on military or any other hostile use of methods and means influencing the infosphere). Не вина Российской стороны, что эта конвенция, постоянно обсуждавшаяся в комитетах ООН, и последующая её активность в области обеспечения международной информационной безопасности, не привели к конструктивному результату, последствия чего мы можем наблюдать в международном взаимодействии.

Почти тремя годами позже после принятия Доктрины ИБ РФ, в США в 2003 году, была подписана «The National Strategy to Secure Cyberspace», вслед за которой в европейских странах на протяжении ряда лет были приняты аналогичные документы с ключевыми словами «Cyber Security». В отличие от Доктрины, где была сделана попытка интегрировать различные аспекты ИБ, они, конечно, были более актуальными в смысле перспектив технической реальности, но имели преимущественно организационно-технологическую направленность, гуманитарный аспект присутствовал разве что декларативно.

Интересна также в связи с этим процессом на Западе история с проектом «Стратегии кибербезопасности Российской Федерации», которая активно обсуждалась и продвигалась в 2012-2013 годах под справедливым лозунгом обновления действующей Доктрины и впечатлением её активистов от принятых в Западных странах документов. К счастью, на наш взгляд, этот вторичный, не суверенный документ с технологическим акцентом, концептуально явно подменявший действующую Доктрину, остался проектом.

Надо сказать, что в общественно-политических условиях 2000 года принятая Доктрина отнюдь не всеми приветствовалась. Так, например, даже не говоря о многочисленных критических высказываниях, в том числе, справедливых, практически одновременно была обнародована так называемая «Белая книга информатизация России», в концептуальном отношении радикально отличавшаяся от параллельной Доктрины.

По горячим следам этих документов нами была предпринята довольно смелая попытка на их основе, воспользовавшись неожиданным структурным подобием принятой Доктрины и разработанной нами модели анализа рисков, провести их количественный анализ для оценки значимости угроз и результативности средств противодействия им.

Новая версия Доктрины, сохранив стратегическую направленность, концептуальную преемственность и комплексность понимания проблем ИБ, в то же время существенно отличается от старой. Прежде всего, это касается целеполагания, что делает её, несмотря на обобщённый характер и сложную структуру, тем не менее, более свободной для применения и в то же время более конструктивной, так как она содержит, по сути, явным образом сформулированные критерии выполнения.

В докладе будет представлен сравнительный анализ структуры старой и новой версий Доктрины ИБ, перспективы её применения в условиях быстро изменяющеёся технологической реальности, а также результаты моделирования 16-летней давности для разных сценариев её выполнения, в частности, с использование положений «Белой книги», а также современные оценки итогов выполнения утратившей силу Доктрины.

УДК 338.2

Ячменева Валентина Марьяновна,
д.э.н., профессор
Ячменев Евгений Федорович,
к.э.н., доцент
Институт экономики и управления
ФГАОУ ВО «Крымский федеральный
университет им. В.И. Вернадского»
г. Симферополь, Республика Крым

СОВРЕМЕННЫЕ ПОДХОДЫ К ОЦЕНКЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА

Управление экономической безопасностью систем различного назначения и уровня иерархии осуществляется через соответствующую систему управления. Определение понятия «система управления экономической безопасностью» приводится во многих работах. В дальнейшем под системой управления экономической безопасностью будем понимать организованную государством совокупность субъектов: государственных органов, общественных организаций, должностных лиц и отдельных граждан, объединенных целями и задачами относительно защиты национальных интересов, которые осуществляют согласованную деятельность в границах законодательства Российской федерации. Основными функциями указанной системы являются: создание и поддержка в готовности сил и средств обеспечения национальной безопасности; управление деятельностью системы обеспечения национальной безопасности; осуществление плановой и оперативной деятельности относительно обеспечения национальной безопасности; участие в международных системах безопасности.

Реализация работ по основным направлениям обеспечения экономической безопасности региона должен предшествовать комплекс мер по оценке достигнутого уровня безопасности, осуществлять который можно с помощью мониторинга.

Управление экономической безопасностью предполагает проведение мониторинга соответствующих процессов, которые идентифицируют систему показателей экономической безопасности. Мониторинг – это информационно-аналитическая постоянно действующая система наблюдений за динамикой показателей, характеризующих экономическую безопасность региона. В современных условиях переходного состояния экономики роль регулярного всестороннего, объективного мониторинга особенно велика, поскольку имеют место высокая подвижность экономических, социальных показателей-индикаторов, наличие многочисленных диспропорций, требующих постоянного внимания. Если мониторинг не отличается высоким качеством, то динамика отрицательных экономических и социальных тенденций, их возникновение и развитие могут выйти из-под контроля, стать неуправляемыми и, в определенной степени, необратимыми. Результаты мониторинга применяются для прогнозирования ситуации в регионе, для управления и при разработке механизма устранения угроз с целью укрепления экономической безопасности, который должен включать критерии и параметры, пороговые значения показателей-индикаторов экономических и социальных процессов.

Решающее значение для обеспечения экономической безопасности региона имеет предупреждение зарождающихся угроз, а не пассивное следование результатам их воздействия. Иначе говоря, предупреждение возникновения угроз экономической безопасности региона не менее важно, чем реализация мер по ликвидации их последствий.

Рассмотрим существующие подходы к формированию такой системы показателей, встречающиеся в различных источниках по проблеме экономической безопасности. При этом следует отметить, что ученые не определились в выборе единого подхода к её формированию.

Так, в ряде публикаций предлагается классифицировать показатели экономической безопасности по ряду признаков. В качестве признаков классификации выбираются: уровень объекта; степень значимости показателей; период действия угроз; направление воздействия на экономику; состав угроз, характер и масштаб вероятного ущерба от их воздействия; подсистемы национальной экономики.

В зависимости от уровня объекта выделяют показатели экономической безопасности, характеризующее мировую экономику, экономику отдельного государства, отдельного региона или отрасли, отдельных предприятия, учреждения или организации, отдельной семьи и личности.

В работе Сенчагова В. О. «О сущности и основах стратегии экономической безопасности России» предлагается ресурсный подход. Согласно которому, качественную оценку экономической безопасности предлагается осуществить по таким показателям: ресурсный потенциал, уровень эффективности использования материальных, финансовых и трудовых ресурсов, конкурентоспособность экономики, целостность территориального и экономического пространства, степень независимости и суверенности государства, уровень социальной стабильности и др. Однако главным недостатком ресурсного подхода является то, что отсутствует точное указание в отношении того, какие из приведенных показателей использовать для оценки конкретной сферы.

В работе Олейникова Е. А. «Основы экономической безопасности (государство, регион, предприятия)» используется иерархический подход. Согласно которому, в зависимости от значимости выделяются общие, базовые и частные макроэкономические показатели, а также дано их подробное описание. Так, к общим макроэкономическим показателям относят такие агрегированные показатели: уровень и качество жизни, уровень инфляции, темпы роста промышленного и аграрного производства, уровень цен, соотношение между ценовой массой товаров и их денежным обеспечением, дефицит бюджета, государственный долг, встроенность в мировую экономику, деятельность теневой экономики. В группу базовых показателей включены: структура собственности, динамика приватизации предприятий, показатели фондового рынка, монополизация и демонополизация, развитие рыночных структур, механизм управления, налоговая система, денежное обращение.

Дарнопых Г. тоже придерживается иерархического подхода и выделяет внутренние факторы экономической безопасности, характеризующие внутренне состояние региональной экономики и внешние факторы, характеризующие связь региональной экономики с внешней средой. Преимуществом иерархического подхода является возможность оценить экономическую безопасность на каждом уровне иерархии. Однако данный подход является качественным и не может дать полную оценку экономической безопасности региона или другого уровня иерархии.

Таким образом, анализ существующих подходов к формированию системы показателей экономической безопасности систем различного уровня иерархии позволяет заключить, что окончательный выбор перечня показателей такой системы в значительной мере зависит от объекта исследования, а также от поставленных целей.

В общем случае анализ системы показателей экономической безопасности подразумевает определенную её оценку, которая может быть осуществлена как качественными, так и количественными методами. Однако, несмотря на то, что качественные методы широко используются для анализа экономической безопасности. Их применение принесет наибольший эффект только в сочетании с количественными методами. В трудах различных авторов встречаются такие подходы к количественной оценке экономической безопасности систем различного уровня иерархии: мониторинг соответствующих процессов, которые идентифицируют систему показателей экономической безопасности и сравнение их с пороговыми значениями; использование методов экспертной оценки, анализа и обработки сценариев; теории катастроф; многомерного статистического анализа.

Апатова Наталия Владимировна
д.п.н., д.э.н., профессор
Сейтвелиев Азиз Арсен угли
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНА

Проблемы информационной безопасности территорий связаны с решением нескольких задач и обусловлены рядом факторов.

К задачам следует отнести обеспечение региона различными видами связи, в том числе, мобильной и Интернет; возможность обращения граждан к органам власти через компьютерные сети и сайты государственных услуг; компьютерная грамотность населения, умение пользоваться электронной почтой и поиском в Интернет; общее состояние региональных СМИ, их распространенность среди населения и доверие к транслируемой информации; доступность органов государственной региональной и муниципальной власти для обращения граждан через различные коммуникационные средства; общий уровень образования населения, готовность к освоению новых знаний и технологий.

Факторы, влияющие на информационную безопасность региона, можно условно разделить на внешние и внутренние. Внешние обусловлены степенью влияния иностранных СМИ, в том числе, сведений, поступающих из компьютерных сетей, на сознание население, его политические и социально-экономические настроения и поведение. Внутренние факторы информационной безопасности зависят от институциональной среды, распространенных в регионе традиций, используемого языка и степени понимания государственного языка – русского, а также от общего социально-экономического положения в регионе, уровня жизни, готовности сохранять целостность региона и государства или добиваться явной, или скрытой автономии в развитии. Стремление жителей региона к устойчивому инновационному развитию, росту благосостояния, повышает уровень информационной безопасности, поскольку не оставляет времени и места для получения и обработки различной отвлекающей от основных целей информации. Повышение собственного образовательного уровня, участие в общественной жизни, постоянная занятость на производстве и в быту создает здоровую моральную обстановку, занятия спортом дают возможность физического совершенствования. В развитых странах организована постоянная пропаганда здорового образа жизни, отдыха на свежем воздухе, участия в местных праздниках и акциях, что также в неявной форме позволяет противостоять информационным угрозам, поскольку люди считают свою жизнь правильной, приносящей моральное и материальное удовлетворение и не хотят менять ее под влиянием чужой, приходящей извне, пропаганды.

Для России и ее регионов в качестве основных направлений создания системы коллективной информационной безопасности, в соответствии с концепцией Евразийской национальной безопасности определены: 1) реализация конституционных прав и свобод граждан в сфере информационной безопасности; 2) совершенствование и защита информационной инфраструктуры; 3) противодействие угрозе развязывания противоборства в информационной сфере; 4) ограничение доступа к информации, содержащей пропаганду террористической, экстремистской и преступной деятельности, травмирующей личность информации, особенно в отношении несовершеннолетних; 5) создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации; 6) разработку, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения. Гарантией выполнения данных задач является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 09.09.2000 г. № 1300.

УДК 330

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

ИНФОРМАЦИОННАЯ ПРОБЛЕМА В ИНВЕСТИЦИОННОМ ПРОЕКТИРОВАНИИ

Информация является важнейшим ресурсом предпринимательской деятельности (фактором производства), наличие достоверной информации - необходимое условие принятия обоснованных управленческих решений. Без информации невозможен процесс управления. В то же время в управленческой деятельности существуют проблемы неполноты, неточности, дефицита, искажения, утечки информации, которые, несмотря на научно-технический прогресс, на развитие компьютерной техники, не уменьшились в последнее двадцатилетие, а, наоборот, только усилились. Данный парадокс можно объяснить высокими темпами изменений в экономической среде, усложнением экономических связей и технологических процессов, усилением конкуренции (результат глобализационных процессов), уменьшением времени для принятия управленческого решения, а также резким возрастанием объема существующей информации.

Информационная проблема также актуальна и в сфере разработки и реализации инвестиционных проектов. Одно из основных отличий проекта от обычной (операционной) деятельности предприятия состоит в его однократном (нециклическом) характере. Каждый проект уникален и требует сбора значительного объема информации, как о внутренней среде проекта, так и о внешней среде. Наиболее сложной задачей в инвестиционном проектировании является задача прогнозирования денежных потоков проекта и ставок дисконта на различные по протяженности временные интервалы (краткосрочные, среднесрочные и долгосрочные проекты). Данное прогнозирование должно базироваться, помимо научно обоснованных методов, на значительном пласте собранной и обработанной достоверной и максимально полной информации.

Наличие достоверной и полной информации – залог принятия правильного решения относительно необходимости реализации инвестиционного проекта. Существует мнение, что даже применяя менее точные методы оценки, но, используя более полную и точную информацию, можно принять более обоснованное решение. А применение сложных методов оценки при условии использования неточной и неполной информации не приведет к положительному результату. Поэтому в инвестиционном проектировании очень важно уделять внимание уточнению используемых данных (разумеется, учитывая отведенный временной интервал для принятия решения и затраты на получение необходимой информации).

Информационная проблема сопровождает проект на всех этапах его осуществления: от зарождения идеи до ликвидации проекта. Идея инвестиционного проекта – результат обработки информации об окружающей среде (экономической, социальной, технологической и др.). Предпринимателю важно обладать стратегическим видением, то есть замечать тенденции развития бизнеса и вовремя на них реагировать. В настоящее время хорошая идея – редкость. В высокоразвитых странах хорошая идея в большинстве случаев может быть реализована, и если не за счет собственных ресурсов ее автора, то за счет заемных или привлеченных средств. А в нашей стране, к сожалению, многие хорошие идеи так и не нашли своей реализации, и мигрировали за рубеж (в США и другие развитые страны).

На этапе разработки проектных материалов и принятия инвестиционного решения идет процесс постоянного сбора и уточнения информации. Сначала, как правило, проводят предварительную оценку эффективности инвестиционного проекта, которая не требует проведения глубокого исследования. Но если проект оказался эффективным на данном этапе, то в дальнейшем начинается процесс уточнения данных.

На этапе реализации проекта проводится его мониторинг, то есть сравниваются фактические данные осуществления проекта с запланированными показателями, выявляются причины подобных отклонений и разрабатываются корректирующие мероприятия. На данном этапе на основе поступившей фактической информации даже может быть принято решение о прекращении реализации проекта.

Если проект все же был успешно реализован, необходимо провести его аудит, сделать определенные выводы и полученные результаты обязательно зафиксировать и хранить.

Поскольку данная информация (особенно если речь идет о проектах крупных компаний) может пригодиться в будущем для реализации следующих инвестиционных проектов.

При этом на всех фазах жизненного цикла проекта существует проблема защиты информации, используемой в проекте (проблема защиты коммерческой тайны), которая усложняется тем, что в проекте, как правило, задействовано большое число лиц и организаций. В ходе осуществления инвестиционного проекта требуется разработка и реализация определенной системы защиты и санкционированного доступа к информации, а также механизм юридической защиты. Так, например, разработанные в рамках проекта новые технологии, продукция, торговые марки необходимо срочно превратить в объекты авторского права.

Выбор программного обеспечения для оценки эффективности инвестиционных проектов также можно отнести к информационной проблеме. Также в инвестиционном проектировании существует проблема различного восприятия одной и той же информации различными субъектами. А для того, чтобы проект успешно реализовать, необходимо достичь определенного согласия между вовлеченными участниками.

УДК 330

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

УПРАВЛЕНИЕ РИСКАМИ ИНВЕСТИЦИОННОГО ПРОЕКТА

Риск является неотъемлемой частью предпринимательской деятельности. Реализуемые на практике инвестиционные проекты (ИП), в которых удается полностью избежать риска, являются крайне редкими и, как правило, не предусматривают возможности получения высокой прибыли. Чем более прибыльным может быть ИП, тем с более высоким уровнем риска он связан. Поэтому управление рисками ИП является неотъемлемой составляющей процесса управления проектами. Вышесказанное особенно актуально для экономики Российской Федерации, которая является нестационарной. Реализация определенного ИП в условиях отечественной экономики является более рисковой, чем реализация аналогичного проекта в высокоразвитых странах Запада.

Под **инвестиционным проектом** понимают какой-либо проект, который основывается на осуществлении инвестиций. Наиболее точным определением термина «риск» считаем определение, данное В. В. Витлинским в монографии «Аналіз, оцінка і моделювання економічного ризику»: «**Риск** – это экономическая категория, которая отображает характерные особенности восприятия заинтересованными субъектами экономических отношений объективно существующих неопределенности и конфликтности, имманентных процессам целеполагания, управления, принятия решений, оценивания, которые обременены возможными угрозами и неиспользованными возможностями».

Управление рисками ИП заключается в предвидении и нейтрализации возможных событий, которые могут привести к негативным финансовым последствиям для инвестора. К основным принципам осуществления этого процесса относят: 1) осознанное принятие риска; 2) способность управлять принятым риском; 3) сопоставимость финансовых возможностей предприятия с принятым уровнем риска; 4) учет временного фактора; 6) соответствие финансовой стратегии предприятия; 7) возможность передачи принятого риска.

Учитывая вышеперечисленные принципы, на предприятии разрабатывается политика управления рисками – это часть всей финансовой стратегии предприятия, целью которой считается разработка системы мероприятий по нейтрализации негативных последствий рисков, связанных с инвестиционной деятельностью.

Инвестиционный проект может характеризоваться различным уровнем риска. Так, например, вероятность неэффективной реализации проекта, равная 0,15, соответствует незначительному уровню риска, а 0,8 – высокому уровню риска.

В процессе управления рисками ИП выделяют следующие этапы: 1) анализ ситуации, то есть должна быть исследована ситуация риска в технической, юридической, финансовой сферах, которые могут либо ограничивать, либо изменять цели ИП; 2) определение возможных видов

риска – на этом этапе необходимо найти, перечислить и охарактеризовать все виды рисков, которые могут повлиять на реализацию ИП; 3) оценка рисков – ранжирование рисков по вероятности наступления или размеру возможного ущерба и их оценка; 4) выбор наиболее приемлемого метода управления риском; 5) реализация принятых решений; 6) оценка эффективности принятых решений.

Для управления рисками существуют следующие основные методы: 1) уклонение/избежание – данный метод считается самым простым, потому что состоит лишь в отказе от осуществления определенных операций; 2) предупреждение/контроль возможных потерь – выполнение таких действий, которые способны снизить и держать под контролем негативные последствия наступления рискового события; 3) принятие риска на себя, то есть готовность компенсировать все возможные потери за свой собственный счет (в основном, для этого создаются специальные фонды и резервы); 4) перенос/передача риска – передача риска другим субъектам, например, страхование (перераспределение риска между группой предпринимателей), хеджирование (подписание договора на куплю/продажу чего-либо в будущем по определенной цене), диверсификация (расширение ассортимента выпускаемой продукции или освоение новых видов ее производства).

Принимая решения относительно реализации какого-либо инвестиционного проекта необходимо учитывать все возможные риски и их последствия. Основываясь на объективных условиях, субъективных предпочтениях, здравом смысле и тщательном анализе имеющихся данных нужно выбрать адекватную стратегию управления рисками ИП, которая обеспечит достижение поставленных целей. Можно сказать, что управление рисками ИП – это не только наука, но также в какой-то степени искусство. Также принимая управленческие решения следует помнить о необходимости применения научно обоснованных методов оценки уровня риска ИП.

УДК 004.056

Бойченко Олег Валерьевич
д.т.н., профессор
Бондарь Вадим Викторович
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ ПЛАТЕЖНЫХ КАРТ

Введение. Развитие информационной безопасности особо актуально в современных условиях бурного развития платежных карт и перехода к автоматизированной системе бухгалтерского учета.

Сегодня банки вынуждены защищать себя от всех возможных рисков как криминального, так и не криминального характера.

Сложность информационной безопасности определяет не только огромные объемы данных, подлежащих обработке и утонченности инструментов, используемых хакерами для доступа.

Это характеризуется тем, что банки, в рамках единой финансовой системы государства, должны соответствовать требованиям безопасности.

Международный опыт по реализации программ карточных платежных систем в разных странах показал, что развитие хакерских методов и способов при соблюдении определенных законов, а также преступления в сфере банковских карточек развивается одновременно с карточной индустрией.

Таким образом, для кредитных организаций в целях обеспечения защиты информации имеет первостепенное значение, что сводит к минимуму потерю денег, и риски банка.

Цели и задачи исследования. Целью данной работы является краткая характеристика безопасности платежных карт.

В соответствии с этим были поставлены следующие задачи: 1. Провести анализ статистических данных по различным видам мошеннических операций; 2. Изучить основные виды мошенничества; 3. Выявить основные виды безопасности платежных карт; 4. Провести анализ путей усовершенствования системы банковских карт.

Методика исследования. В качестве методов, применяемых для исследования данной темы, будут использованы теоретический анализ литературы и материалов сети Интернет, выделение главных элементов, обобщение.

Результаты исследования. В 2014 году, по мнению экспертов, произошло быстрое развитие вредоносных программ для банкоматов.

Они имеют широкие функциональные возможности - от получения деталей банковской карты для снятия наличных и несанкционированного доступа к внутренней сети банка.

Не теряет популярность и «классический» скимминг.

Анализ сводных данных по разработке безопасных приложений и оценке уязвимостей позволяет установить следующее:

- в 2014 году злоумышленник в 9 случаях из 10 смог получить доступ к внутренним узлам сети субъекта национальной платежной системы, а в 2012 году в подобное соотношение составило 7 из 10;
- для осуществления нападения, в 82% случаев, достаточно иметь средний или низкий уровень квалификации;
- Web-уязвимости приложений исследованных систем выявлены в 93% случаев;
- причины уязвимости связаны с антиблокировочной системной ошибкой (23%), а также с отсутствием эффективных механизмов защиты (43%);
- уязвимости приложений - одна из наиболее распространенных факторов, способствующих проникновению корпоративной сети.

Следует подчеркнуть, что основные методы мошенничества, существующие в Российской Федерации, хорошо известны и существуют довольно давно.

Самый распространенный способ – это небрежность и юридический нигилизм клиентов, которые раскрывают PIN-код, написав его на карту; другой аспект относится из-за, так называемого «дружественного мошенничества», состоящего в раскрытии PIN-кода членам семьи, близким друзьям, коллегам.

Другой пример относится к методам социальной инженерии, когда из-за технических факторов, связанных с неграмотностью клиентов, возникает паника при получении SMS-сообщения «Ваша банковская карта заблокирована» со всеми вытекающими из этого последствиями для них.

Существует также общая схема, чтобы помочь прохожему попасть в так называемую «ливанскую петлю». Суть заключается в том, что при блокировке банковской карты, для оказания помощи клиенту, приходит «добрый» мошенник.

Таким образом, все разнообразие мошеннических схем, в большинстве случае связано с человеческим фактором.

Согласно статистическим данным, из 10 инцидентов в области информационной безопасности только одна учетная запись относится к действиям внешнего «хакера», остальные же (9) касаются действий нерадивых, безответственных и плохо обученных сотрудников предприятия.

Выводы. Можно сделать вывод, что качество обеспечения безопасности банковской карты зависит, прежде всего, от «честности» участников финансовых отношений, эффективности служб безопасности кредитных организаций, профессионализма сотрудников правоохранительных органов, участвующих в предупреждении и выявлении случаев мошенничества в банковском секторе, а также повышении ответственности законных держателей пластиковых карт.

Анализ проблем, связанных с обращением платежных карт, позволил сформировать алгоритм достаточных условий для обеспечения их информационной безопасности:

- детальная разработка нормативно-правовой базы, закрепляющей специфику обращения платежных карт;
- информационная работа среди населения;
- защита информационных ресурсов от несанкционированного доступа.

УДК 004.056.5

Бойченко Олег Валерьевич,
д.т.н., профессор
Институт экономики и управления
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Коротчук Анастасия Павловна,
курсант 2 курса
Крымского филиала Краснодарского университета МВД России

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-БАНКОВСКОЙ СИСТЕМЫ РОССИИ

Осложненное экономическое положение Российского государства является результатом значительного негативного воздействия как западных санкций в адрес России, так и ответных российских мер. Необходимость исследования определяется высоким уровнем преступности в Российской федерации в сфере экономических преступлений, а особенно в кредитно-банковской деятельности.

Согласно статистке, выведенной пресс-службой PwC по итогам 2016 года, Российская Федерация занимает лидирующее место по количеству преступлений в сфере экономики по всему миру (Рис.1.).

При этом наиболее распространёнными преступлениями является незаконное присвоение активов, преступления коррупционного характера и фальшивомонетничество.

Особую нишу в сфере экономических преступлений занимают преступления, относящиеся к кредитно-банковской системе. К ним относятся противозаконные деяния с использование банковских карт, систем дистанционного банковского обслуживания, лжепредпринимательство, злоупотребление депозитным капиталом и злостное уклонение от погашения кредитной задолженности.

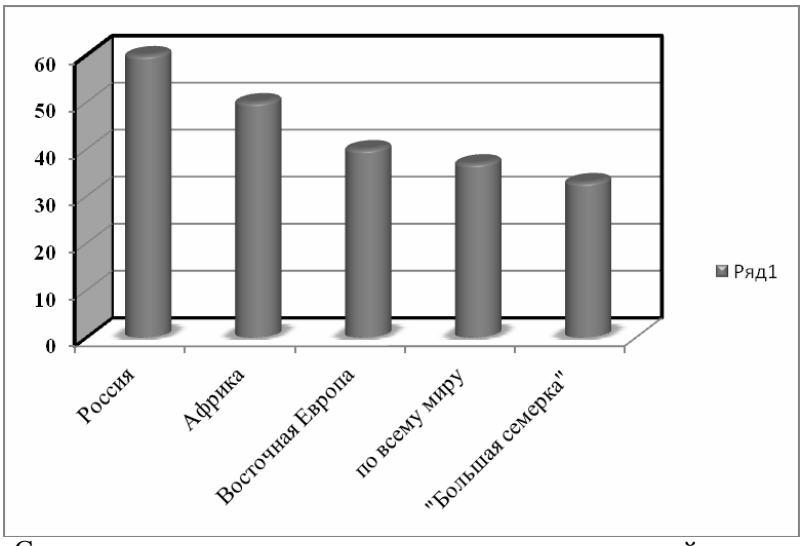


Рис. 1. Сравнительная характеристика уровня экономической преступности

Внедрение компьютерных технологий и электронной техники в систему банковского производства на современном этапе развития общества стало неминуемым.

Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии.

На данный момент в России почти не осталось чисто бумажных банковских процессов. Всю учетно-операционную деятельность российских банков поддерживает комплекс автоматизированных систем, распределенных по региональному принципу в соответствии с действующей банковской структурой. Безналичные деньги, ценные бумаги, договоры – все храниться в электронном виде. Например, в Банке Россия действует единая информационно-вычислительная система центрального аппарата, которую используют для сбора и обработки банковской отчетности, и других банковских операций. Так, почти в каждом из 78 территориальных учреждений Банка России созданы свои информационно-телекоммуникационные системы (ИТС), без которых работа любого банка сейчас не реальна. При этом такая система подверженная повышенному риску возможности взлома сайтов

хранения информации, что приводит к утечке конфиденциальных данных о клиентах, товарах, ценах.

Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий.

В настоящее время свыше 90% всех преступлений в банковско-кредитной сфере происходит с помощью технического оборудования.

Нарушителем может быть любой человек из следующих категорий сотрудников:

• штатные пользователи АБС;

• сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение системы;

• обслуживающий персонал (инженеры);

• другие сотрудники, имеющие санкционированный доступ к АИТ (в том числе подсобные рабочие, уборщицы и т.д.).

При этом такая система подверженная повышенному риску возможности взлома сайтов хранения информации, что приводит к утечке конфиденциальных данных о клиентах, товарах, ценах.

Безопасность информации напрямую влияет на уровень рентабельности банка, ибо потери, связанные с нарушением целостности Автоматизированной Банковской Системы, могут свести на нет все достижения эффективного управления.

Последствиями преступной деятельность могут быть не только повреждение технического оснащения банка и финансовые потери, а так же имиджевые и юридические издержки.

Компьютеризация банковской деятельности продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий.

Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный уход на безналичные расчеты с использованием пластиковых карт, сети Internet и удаленных терминалов управления счетом юридических лиц.

В связи с этим следует ожидать дальнейшее динамичное развитие средств информационной безопасности банков, поскольку их значение постоянно возрастает.

Поэтому, взаимоинформированность сотрудников правоохранительных служб и банковских служащих, а так же иных работников финансовой сферы, позволит проводить эффективные мероприятия по раскрытию, пресечению и предотвращению экономических преступлений, и укреплению общефедеральной экономической безопасности.

Данное сотрудничество так же позволит выявлять факторы внешней и внутренней дестабилизации экономической деятельности хозяйствующих субъектов, разрабатывать и реализовывать конкретные меры по своевременному выявлению рисков и установлению причин и условий, способствующих незаконным финансовым потерям.

УДК: 32.019.51

Boychenko Oleg Valerievich
Doctor of Technical Sciences, Professor
Korshunova Irina Grigorievna
Senior teacher
Krasnodar University of Interior, Crimean Affililiate

MAJOR PROBLEMS OF INFORMATION SECURITY AND POSSIBLE SOLUTIONS

One of the problems facing organizations or institutions is information security. There are still many problems businesses must overcome in the need truly protect data from occasional hackers as well as main cybercriminal groups. Moreover, data intrusions continue to happen in all industries and productions, and the general occurrence of these cyber attacks is not decreasing despite the great number of cyber security disputes.

Threats to any computer network appear from both external and internal intrusions. External threats include unauthorized access by outsiders such as hackers, virus attacks etc. Among internal threats is exploitation of the network by its users – intentional or non-intentional. Internal threats occur due to malicious intentions or ignorance of the users of computer network. For example, a person can leave the computer unattended exposing it to others who are not authorized to access the information. Another example of internal threat can be a person downloading something from the Internet that results in a malicious software attack.

According to analysis of the foreign Internet sights, the information security challenges have been identified as follows:

- Compromised devices and credentials. Malicious software has dramatically evolved and become more complicated and dangerous than before. That is why business leaders must take preventive measures to update their information security standards.

As George Kurtz told Computer Business Review at InfoSec 2016 "If you're looking for malware you won't see breaches using legitimate credentials".

Hackers steal login information and use credentials to access applications and information they are interest in. Consequently, it's difficult to identify when organizations are intruded. As a result, many organizations lose their data and find out about penetrations some time later.

To overcome this information security challenge it is necessary to try a new role based approach to estimate control.

Second challenge is hacker movement breach restriction.

Once cybercriminals find their way inside corporate networks, they're moving laterally between applications until they find the most vulnerable and valuable data. In this case cryptographic isolation and end-to-end encryption prevents lateral movement.

Microsegmentation technologies must be applied for enterprise security. The research firm explained that if workloads isolated cryptographically, organizations can prevent hacker movement, contain intrusions and better secure data.

The third problem has been identified by Stuart Clark as "security Frankenstein". It means that by using mismatched security decisions instead of one intergral product, organizations put data at risk. In the view of above, businesses and associations should try and identify single cybersecurity solution that effectively corresponds all needs. It includes cryptographic segmentation and role-based access control that corresponds all information security requirements.

Cloud computing and big data have become the norm for many organizations nowadays. However; with this comes the proliferation of unsecured data passed between users and applications, leaving lucky chances for hackers to take a use.

One more problem can arise with the following point: ignoring the problem won't make it go away. As a result, it will leave organizations operating much less effectively.

A more sufficient policy is to focus on reducing the attack surface, which can be achieved through application segmentation, a form of IT compartmentalization.

We take the term «compartmentalization» involves shifting the focus from stopping breaches to containing them. It's a well-known fact that penetrations will occur. That is why by segmenting the IT environment the compromised systems can be identified faster and the damage can be softened.

It is a true fact that compartmentalization is a tried concept from ship-building. Creating water-tight compartments with bulkheads in a ship's hull will ensure the ship stays afloat when a breach of the hull happens. Similarly, application segmentation provides compartmentalization of enterprise IT. It, and means that when the inevitable cyber-breach occurs, the organization is not put at risk.

Nowadays, compartmentalization can be employed through crypto-segmentation, which can be put into practice as follows:

1. Security groups to base segmentation on business applications and grant access based on user roles. These ideas can be easily put in place as crypto-segmentation operates at the application layer, rather than at the infrastructure layer.

2. Intrusions to be effected even when the attacker works in the company, since insiders are restricted to only the segments, departments for which they are authorized.

Factually, penetrators generally become effective insiders when they successfully compromise user credentials through phishing and spear-phishing. So crypto-segmentation contains these attackers and constrains their movement even when phishing attacks have reached their targetl.

3. Attacks must be prevented as well as the damage. If attackers realize that violation an organization's security does not give much profit, their focus of attention will be shifted elsewhere. It can be compared to the homeowner who knows that a proper alarm system set to secure the property will diminish the risk of possible burglary. Furthermore, a hacker who finds that his access is limited and prohibited will strive to less secure companies.

Crypto-segmentation is available today and promotes to install business-driven security, aligning security controls to business objectives instead of infrastructure's limitations.

УДК 65.011.12

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

ПРИМЕНЕНИЕ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ В РЕСПУБЛИКЕ КРЫМ

В связи с введением организации предоставления государственных и муниципальных услуг в единой информационной системе было принято постановление в мае 2016 года о создании Региональной системы межведомственного электронного взаимодействия (СМЭВ) Республики Крым.

Данная система представляет собой базу данных о программных и технических средствах, которые используются для возможности доступа через систему взаимодействия к информационным системам государственных организаций. Также в ней содержатся сведения об истории передвижения электронных сообщений в СМЭВ.

Каждый регион до применения системы межведомственного электронного взаимодействия подготавливает электронный сервис, в котором каждый поставщик данных способен верно обработать запросы и своевременно выдать сведения, а каждый потребитель сумеет правильно задать запрос на сведения и получить ответ.

Для отправки электронных сообщений используется протокол доступа к объектам Simple Object Access Protocol (SOAP). Чаще всего он используется поверх протокола передачи гипертекста HyperText Transfer Protocol (HTTP).

Для защиты и проверки персональных данных на первоначальном этапе используется протокол целостности и конфиденциальности Web Services Security. Основным направлением деятельности является использование XML Signature. Таким образом пользователь во время входа проходит аутентификацию с помощью личного сертификата.

Для документооборота используется формат долгосрочного архивного хранения электронных документов PDF/A с размещением реквизитов электронного документа в XML-файле.

Требования к формату и структуре данных описываются в соглашении между организациями (поставщика электронной службы - Министерства внутренней политики, информации и связи Республики Крым и потребителей электронного сервиса - исполнительных органов государственной власти Республики Крым и отнесенных к их ведению государственных организаций, органов местного самоуправления муниципальных образований в Республике Крым, муниципальных организаций, многофункциональных центров предоставления государственных и муниципальных услуг).

В основном используются типовые варианты подключения:

1) Использование продукции «Инфотекс»: использование кластера ПАК HW1000; использование одиночного ПАК HW1000; использование одиночного ПАК HW100 модификаций A/B/C;

2) Использование продукции «Код безопасности»: использование кластера АПКШ Континент IPC-3000; использование одиночного АПКШ Континент IPC-3000; использование кластера АПКШ Континент IPC-1000; использование одиночного АПКШ Континент IPC-1000; использование кластера АПКШ Континент IPC-100; использование одиночного АПКШ Континент IPC-100; использование одиночного АПКШ Континент IPC-25; использование одиночного АПКШ Континент IPC-10;

3) Гибридная схема – симбиоз предыдущих вариантов.

В части криптозащиты со стороны центра управления сетью необходимо обеспечить возможность подключения к сетевому оборудованию поставщика с использованием интерфейсов Ethernet Base T 100/1000.

Также необходимо обеспечить связность на втором уровне модели OSI/ISO внутренних интерфейсов криптошлюзов при кластерном подключении, т. е. разместить два физических интерфейса в одном широковещательном сегменте.

При подключении через сеть Интернет необходимо обеспечить доступность внешнего интерфейса криптошлюза (внешний «белый» IP адрес) из сети Интернет одним из следующих

способов:

- обеспечение NAT-трансляции частного IP-адреса в публичный IP-адрес и публичного IP-адреса в частный по протоколам TCP, UDP и портам (55777, 500, 4433, 4431)
- выделение для интерфейса публичного IP-адреса.

Таким образом, введением системы межведомственного электронного взаимодействия должны быть решены следующие задачи:

1. Повышение качества и доступности предоставления государственных и муниципальных услуг;
2. Обеспечение согласованных и эффективных действий участников информационного обмена, ведущих к сокращению сроков получения результатов предоставления государственных и муниципальных услуг с одновременным повышением их качества

УДК 004.056.03

Бойченко Олег Валерьевич
д.т.н., профессор,
Мамутов Э.Э.
студент 5-го курса бакалавриата заочного отделения
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

ФОРМИРОВАНИЕ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Процесс успешного функционирования предприятий во многом зависит от модернизации их деятельности в контексте обеспечения экономической безопасности.

Экономика, которая находится в состоянии трансформации, требует от всех предприятий, независимо от форм собственности и методов хозяйствования, умения выживать в условиях конкурентной борьбы, приспосабливаться к динамическим изменениям в политике, экономике и обществе в целом.

Успешное функционирование предприятий в условиях меняющейся среды возможно только при наличии системы безопасности (далее СЭБ), задачами которой является прогнозирование значимых событий, реагирование и предупреждения угроз.

Также следует отметить, что для обеспечения безопасной работы предприятия необходимо создание системы комплексной защиты, которая является самостоятельной, обособленной от других систем предприятия, например, производственных.

Но ее обособленность является относительной, так как СЭБ – это сложный элемент управления предприятия в целом.

Универсальных рецептов не существует: СЭБ индивидуальна на каждом предприятии, так как зависит от уникальной совокупности внутренних и внешних факторов.

Основа формирования системы – оценивание уровня экономической безопасности с помощью дерева индикаторов. Ни одна из составляющих дерева индикаторов не имеет преимущества над другими, но одновременно они связаны друг с другом.

Дерево индикаторов может быть представлено картой с многочисленными точками-входами. Но, в тоже время, экономическая безопасность – это многовекторное измерение. Индикаторы (показатели) уровня угроз определяются каждым предприятием на основе видения потенциальных рисков, возможных потерь и вероятности их наступления.

Дерево индикаторов, система фильтров и определенные критические зоны (нормальная, предкризисная, кризисная) для каждого индикатора связаны с деревом решений, которое содержит сценарии развития событий и возможные контрмеры со стороны предприятия.

Причем, каждый вариант решения предполагает конкретных исполнителей для принятия решения и его выполнения (или в рамках собственной службы безопасности, или через аутсорсинг).

При использовании дерева индикаторов эффективность управления значительно повышается вследствие корректности отражения в модели самого объекта безопасности, так как показатели в дереве приводятся по направлениям деятельности предприятия, основным ресурсам или главным рискам.

Использование дерева решений и исполнителей позволит функционировать СЭБ в виде стратегии, то есть позволит проигрывать возможные ситуации при реализации риска или управленческом решении.

Принцип работы подобных адаптивных систем основан на постоянной обработке текущей информации, которая компенсирует недостаток априорных данных.

Проблему оперативного обновления информации в предложенной модели экономической безопасности предлагается решить через возложение функций на ответственных в бизнес-подразделениях предприятия.

Введение оперативной информации необходимо производить с логически оправданной периодичностью, при этом, частота введения данных определяется для каждого бизнес-подразделения индивидуально.

Функционирование адаптивной (гибкой) системы безопасности происходит через разделение сложной задачи на более простые, путем выделения процессов на уровне центров ответственности (бизнес-подразделений), для которых и решаются оптимизационные задачи.

При получении решений простых задач решается оптимизационная задача в совокупности по конкретному уровню экономической безопасности. Далее с использованием полученных решений-выигрышей решается оптимизационная задача на уровне экономической безопасности предприятия.

В целом система формируется по приведенному алгоритму, но с учетом индивидуальности каждого предприятия.

Данные для оценки показателей вносятся в базу сотрудниками финансово-экономического отдела, или автоматически переносятся из стандартных форм финансовой отчетности.

Оценка таких объектов безопасности, как имидж предприятия предполагает использование метода экспертных оценок, позволяющего перевести качественные показатели в количественные.

Предприятие само определяет экспертов по каждой составляющей дерева индикаторов, содержание опросников (Check lists) и периодичность анализа.

Точкой принятия решения на предложенной схеме является достижение показателем финансовой устойчивости кризисного уровня.

Хотя алгоритмом может быть предусмотрен мониторинг не только обобщающего показателя, но и отслеживание уровня каждого из составляющих показателей, соответственно, точка принятия решения будет раньше.

Анализируются не только фактические показатели деятельности предприятия, но и прогнозные значения отдельных факторов. Мониторинг вероятных изменений законодательства, тенденций НТП и т.д. дает возможность предупредить возможные угрозы, и позволяет системе своевременно адаптироваться.

Динамичность полученной системы экономической безопасности обеспечивает постоянный анализ индикаторов экономической безопасности, определение критических зон, возможность мониторинга состояния экономической безопасности в целом и по отдельным направлениям. А возможность быстрого выбора оптимального решения придает системе адаптивности к меняющимся условиям.

Предложенная система позволяет быстро принимать решения и реагировать на изменения, она чрезвычайно эффективна в условиях нехватки времени/средств на получение дополнительной информации. Однако, нужно учитывать непредсказуемые угрозы, соответственно, рассматривать представленный подход к обеспечению экономической безопасности как инструмент. Для актуальности системы нужно ее периодически просматривать как в целом, так и по отдельным составляющим.

УДК 004.056.53

Бойченко Олег Валерьевич
д.т.н., профессор,
Серафимова Анастасия Александровна
студентка 4 курса бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КАДРОВЫЕ ПРОБЛЕМЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Киберпреступность сегодня характеризуется постоянно возрастающим количеством утечек конфиденциальной информации. Согласно исследованиям Meridien, потери только от Интернет-мошенничества достигнут к 2017 году 15–45 миллиардов долларов США. Существенное противодействие росту преступлений в сфере информационных технологий

может оказать грамотная политика подготовки национальных кадров в сфере информационной безопасности.

Так, в первом полугодии 2016 года аналитическим центром InfoWatch зарегистрировано 723 случая утечки конфиденциальной информации в мире, что на 10 % превышает все показатели 2015-го года. Угрозы информационной безопасности становятся не только все более распространенными, но и выходят на качественно новый уровень.

По шкале от 1 до 5, где 5 наивысший балл хотелось бы привести данные о киберприступности на рынке.

С другой стороны, рынок информационной безопасности характеризуется всевозрастающим спросом, работодатели готовы на все, дабы сохранить ценных сотрудников. Не исключено повышение заработной платы в среднем на 30 %.

Большинство экспертов и аналитиков называют сферу информационной безопасности наиболее востребованной и перспективной с профессиональной точки зрения на ближайшее будущее.

Необходимость в специалистах данной отрасли по прогнозам должна вырасти на 36, 5 % уже к 2022 году

Цель исследования состоит в изучении проблематики кадровой составляющей в сфере обеспечения информационной безопасности при функционировании автоматизированных управляющих систем в экономической деятельности.

Проблемы информационной безопасности уже не является исключительно сферой компетенции специальных служб (государства), они все больше становятся предметом внимания общества и личности.

На сегодня Министерством образования России совместно с заинтересованными федеральными органами исполнительной власти создана основа государственной системы подготовки специалистов с высшим образованием, способных решать задачи обеспечения ИБ стран.

Подготовка специалистов в сфере информационной безопасности в РФ имеет 50-летнюю историю (сегодня более 115 вузов России осуществляют подготовку специалистов по указанной специальности).

В России вопросы подготовки кадров по информационной безопасности в национальном масштабе получили развитие в 1992 г., когда была сформирована межвузовская научно-техническая программа «Методы и технические средства обеспечения безопасности информации». В период между 1992 и 1998 гг. сложился крупный коллектив исполнителей, в состав которого вошли 15 крупнейших вузов России, главным среди которых стал Московский инженерно-физический институт (МИФИ). Интернациональный характер проблемы государственного обеспечения защиты информации требует консолидации и координации усилий всех стран в плане подготовки специалистов по защите информации.

К 2019-тому году ожидается, что спрос на рабочую силу в данной отрасли вырастет на 6 миллионов вакансий, при том, что прогнозируемый дефицит - 1,5 миллионов специалистов. Дефицит специалистов в сфере информационной безопасности есть во всем мире.

Прогнозы доказывают, что примерно есть 1 миллион незакрытых вакансий.

Директора по информационной безопасности испытывают существенные трудности в процессе реализации профильных проектов, обусловленные нехваткой знаний и навыков у сотрудников (34,5 %) или просто отсутствием необходимых специалистов на предприятии (26,4 %).

Учитывая такие данные, лишь малое количество предприятий может предоставить полноценную, комплексную защиту внутренних информационных ресурсов собственными силами (24 %).

Эта проблема решаема, но требует времени и не малых усилий. Поиск решения данной проблемы упирается не на биржу труда, а на студенческую аудиторию.

Сегодняшние ученики профильных вузов – это будущие специалисты, которые помогут решить существенные трудности.

Но данная цель будет достигнута лишь в том случае, если уровень их знаний будет достаточно высок.

Также нужно учесть тот фактор, что успешно пройти необходимую подготовку получится с условием того, что на пути обучения и освоения сего дела, повстречаются люди, которые помогут и объяснят, как это быть асом в своем деле.

Предприятия, которые занимаются разработкой программного обеспечения в сфере информационной безопасности, должны понимать, что их будущее, зависит от того, готовы ли они делать вклад в обучение молодых специалистов и принимать в этом непосильные участие.

Студенты остро нуждаются в практике. Лишь практические навыки помогут студенту быстрому освоение данного дела.

Практика даст понимание того, как должен работать профессионал и на каких принципах должна будет основываться его деятельность.

Предприятиям данной отрасли не мешало б иметь партнерские отношения с учебными заведениями, дабы быть своеобразным экскурсом в профессию для тех, кто лишь начинает свой путь.

Таким образом, из вышесказанного можно сделать вывод, что спрос на специалистов существенно превышает количество кандидатов, потому, лишь от компаний, работающих в данной отрасли зависит, кто будет занимать свободные должности и что будет в дальнейшем.

В заключение можно сказать, что борьба с компьютерной преступностью и кибертерроризмом является одной из важнейших задач современности.

Насущной задачей современного образования становится разработка таких методов учебно-воспитательной работы, где бы гармонично сочеталось обучение современным информационным технологиям с формированием высоких нравственных качеств для выработки иммунитета к совершению компьютерных преступлений.

Успешность противодействия в этом направлении во многом определяется качеством подготовки специалистов по информационной безопасности. Совершенствование учебно-воспитательной работы создает предпосылки для предотвращения и предупреждения компьютерной преступности, особенно, в молодежной среде

УДК 004.056.04

Бойченко Олег Валерьевич,
д.т.н., профессор,
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Табакару Елена Юриевна,
курсант 3 курса,
Крымского филиала Краснодарского университета МВД России
Симферополь, Россия

ПЕРСПЕКТИВЫ ВИРТУАЛЬНОЙ БЕЗОПАСНОСТИ В РОССИИ

Введение. В наши дни, учитывая прогресс информационных технологий и динамику количества пользователей виртуального пространства, появились различные способы использования киберпространства, что является целью совершенствования преступных посягательств.

Постановка проблемы. Всемирная сеть «Интернет», показавшая новейшие пути и глобальные возможности для получения информации и обмена ею, совершенствуется очень стремительно. И поэтому в России за последнее время значительно выросло количество компьютерных преступлений, возрастает так же их общее количество по масштабам похищенного и другим видам ущерба в общей доле материальных потерь от обычных видов преступный деяний.

Целью данного исследования является анализ перспектив виртуальной безопасности в России и разработка инновационных подходов решения выявленных проблем.

Методы исследования. Информационная безопасность является ключевым аспектом в развития Российского государства и общества в целом. Глобальное развитие сетей общего пользования и внедрение их во все направления деятельности человека, значительно меняет сущность преступных действий, которые могут принести колоссальный вред политическим, социально-экономическим, научно-техническим, культурным и информационным отношениям.

По полученным данным из ГИАЦ МВД России за 2015 год, по фактам совершения компьютерных преступлений были возбуждены уголовные дела: за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 1396; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 974; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информационно-телекоммуникационных сетей (ст. 274 УК РФ) – 12.

Большинству преступных действий, совершающихся в сетях общего пользования, характерны следующие особенности:

1. Высокий уровень скрытности преступлений, обуславленный особенностью виртуального пространства;
2. Особый территориальный характер сетевых преступлений, при котором злоумышленник, потерпевший и объект преступного посягательства могут находится на территориях разных государств;
3. Особая и масштабно продуманная профессиональная преступная деятельность;
4. Системность, разнообразие, нестандартный подход и появление новых, обновленных путей преступного воздействия на объект посягательства;
5. Возможность совершения преступлений в нескольких местах одновременно;
6. Много эпизодный характер преступных действий при наличии большого количества потерпевших;
7. Неосведомленность пользователей о том, что они стали объектом преступного посягательства;
8. Абсолютная дистанционность незаконных действий в отсутствие физического контакта между злоумышленником и потерпевшим;
9. Невозможность профилактики, пресечения и предотвращения преступных действий.

В Российской Федерации больше всего внимания уделяется понятию «компьютерная преступность». Наверняка это соотносится с тем, что исследования осуществляются в криминалистической или процессуальной сферах деятельности. Необходимо выделить, что в Уголовном кодексе РФ существует ответственность за преступления, объектом преступных посягательств которых является информация и информационные системы под названием «Преступления в сфере компьютерной информации».

Следует подчеркнуть, что понятие «киберпреступность» значительно шире, чем «компьютерная преступность» и более объективно выражает природу такого явления как преступность в глобальном информационном пространстве. Так, «киберпреступность» - это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. При этом, термин «компьютерная преступность» относится только к киберпреступлениям, совершаемым против компьютеров или компьютерных данных.

Структура киберпреступности исходит прежде всего, от характера и степени развития информационных технологий и «погруженности» пользователей в интернет.

Результаты исследования. Во избежание данных нарушений закона необходимо осуществлять контроль как на международном уровне, так как на уровне отдельного государства, так как осуществлять мероприятия по профилактике и борьбе с киберпреступностью почти невозможно.

Следует отметить, что в уголовном законодательстве России ответственность за преступления в сфере компьютерной информации регламентируются главой 28 УК РФ, которая содержит в себе всего три статьи: 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных программ для ЭВМ), 274 (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети).

Таким образом, существующее уголовное законодательство об ответственности за преступления в сфере компьютерной информации направлено исключительно на компьютерные преступления, т.е. преступления, которые совершающихся в отношении компьютеров и компьютерной информации (преступления против компьютерной безопасности), однако не касается других преступлений, совершаемых с их использованием.

Выводы. Представляется целесообразным ввести в УК РФ норму о «приобретении права на чужое имущество, совершенное путем ввода, изменения, удаления или блокирования компьютерных данных либо иного другого вмешательства в функционирование компьютера или компьютерной системы» («компьютерное хищение»). По сути, эта норма будет охватывать деяния, называемые «компьютерными кражами», не подпадающие под действие статьи 158 УК РФ.

УДК 32.019.5

Бойченко Олег Валерьевич,
д.т.н., профессор
Институт экономики и управления
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Шадрина Анастасия Юрьевна,
курсант 1 курса
Крымского филиала Краснодарского университета МВД России
Симферополь, Россия

РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ И ЕЕ РЕГИОНАХ

Постановка проблемы. Постиндустриальное общество в России началось развиваться совсем недавно. Это новый этап жизни общества повлекший за собой глобальные изменения и поставивший в центр внимания такие понятия как информация и знания. На данный момент информационно-коммуникационные технологии являются необходимыми для развития экономической, социально-политической, культурной и духовной жизни общества, конкурентоспособности России и повышения качества жизни её гражданам.

Цель работы заключается в определение основных направлений и первоочередных действий для повышения качества жизни и совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий в России.

Основными целями развития информационного общества являются:

- укрепление федеративного государства.
- создание современных сетевых структур государственного, регионального и муниципального управления.
- становление и в последующем доминирование в экономике новых технологических укладов.
- повышение качества образования.
- повышение роли квалификации, профессионализма и способностей к творчеству как важнейших характеристик услуг труда.
- достижение высокого уровня минимальной социальной обеспеченности;
- создание эффективной системы обеспечения прав граждан и общественных институтов на свободное получение, распространение и использование информации как важнейшего условия демократического развития;
- обеспечение высокого уровня национальной безопасности.

Основные направления развития общества:

- развитие информационно-коммуникационной инфраструктуры.
- формирование условий, способствующих производству и использованию информации и знаний во всех сферах жизни общества. Развитие человеческого капитала.
- развитие информационной среды как базы совершенствования сферы государственного управления .
- обеспечение информационной безопасности страны
- международное сотрудничество в сфере ИКТ.
- совершенствование и развитие нормативно-правового регулирования процессов информационного развития.

Таким образом, первоочередными действиями по развитию информационного общества являются:

- принятие политических, организационных и экономических решений, необходимых для обеспечения приоритетности опережающего информационного развития России;
- принятие руководством страны комплекса мер по укреплению партнерских отношений государства, бизнеса, общественных организаций и населения в реализации стратегии информационного развития;
- ускоренное совершенствование и развитие законодательной и нормативно-правовой базы информационного развития;
- опережающие модернизация и развитие информационно-коммуникационной инфраструктуры, в особенности в отдаленных регионах страны;
- расширение использования ИКТ в образовании и научной деятельности;
- принятие мер по повышению эффективности реализуемых в настоящее время

федеральных, региональных и отраслевых программ информатизации;

- эффективное экономическое стимулирование развития отечественной научной и производственной базы ИКТ.

Основные проблемы развития информационного общества в России:

- неравномерность информационного развития её регионов:
- недостаточное правовое регулирование;
- низкий уровень образования населения в сфере ИТК и недостаток специалистов;
- нестабильность политического и экономического положения в стране ;
- снижение уровня и возможностей централизованного управления ;
- неравномерный доступ людей к информационным благам ;
- формирование личности в информационном обществе;
- недостаточность полномочий управляющих и координирующих органов в сфере ИКТ в субъектах РФ.

Выводы. Движение к информационному обществу — объективный процесс, обеспечивающий формирование и развитие мирового информационного пространства, взаимосвязанное функционирование мировых товарных рынков, рынков информации и знаний, капитала и труда.

В настоящие время Россия движется к развитию информационного общества в каждом уголке страны.

Уже разработаны соответствующие программы, принята и реализуема «Стратегия развития информационного общества в Российской Федерации».

Сформирование современной информационной инфраструктуры в России будет способствовать вхождению страны в мировое информационное сообщество, что обеспечить её конкурентоспособность в глобальном мире.

УДК 336.6

Бондарь Александр Петрович
к.э.н., доцент
Шульга Екатерина Владимировна
Бочарова Алена Олеговна
бакалавры
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

В современном мире инновационная деятельность играет существенную роль для развития экономики государства, ее по праву можно считать одним из наиболее важных факторов развития промышленности в стране. Внедряя новые идеи, новые виды продукции, технологии, ноу-хау в различные области производства, предприятия тем самым повышает свою конкурентоспособность. Эти процессы являются особенно важными для научных и промышленных предприятий. Внедрение нововведений позволяет им определить потребности рынка и быстро отреагировать на запросы потребителей, тем самым повышая свою рентабельности и финансовую стабильность.

Проведение эффективной инновационной деятельности нуждается в наличии соответствующего информационного обеспечения, которое могло бы дать доступ к нужной технической, экономической, научной информации, которая в то же время являлась бы достоверной и актуальной.

Внедрение инноваций требует существенных усилий и ресурсов на всех этапах инновационной деятельности. Информация должна прорабатываться как можно более детально с начальной стадии принятия решений в области инноваций. Чем более обоснованное принимается решение, тем успешнее проходит внедрение новых технологии, продуктов, ноу-хау. Без надлежащего информационного обеспечения успех нововведений бывает случайным, а в некоторых случаях, недооценка определенных факторов вследствие недостаточной информированности является причиной отказа от инновации на более поздних этапах ее реализации.

Важным условием в информационном обеспечении является фактор актуальности. Поскольку информационные процессы растянуты во времени, то достоверная, но устаревшая информация может приводить к ошибочным решениям. Так, обеспечение своевременной и точной информации при осуществлении инновационной деятельности определяют сущность информационного обеспечения.

Специфика информационного обеспечения инновационной деятельности заключается в том, что субъектам инновационной деятельности требуется не только научно-техническая информация, но и также информация о рыночной конъюнктуре в соответствующих сегментах, о патентах и «ноу-хау», о предложениях на научно-технические и экспериментальные услуги и т.д. Таким образом, информационное обеспечение инноваций должно носить комплексный характер.

С учетом нынешней социально-экономической ситуации и обобщая текущие тенденции в области информационного обеспечения инновации и инновационной деятельности, можно констатировать, что в качестве ключевых направлений информационного обеспечения наибольший интерес представляет: инновационная деятельность промышленных предприятий, отраслевых организаций, инновационная деятельность в сфере услуг.

Для инновационно-активных предприятий, прежде всего, нужны базы данных по инновационным разработкам, которые позволяли бы сделать вывод об их рыночных перспективах и возможностях их коммерциализации. Для этого нужны консалтинговые инфраструктуры, способные предоставить необходимую информацию. Взаимодействие с внешними информационными структурами, такими как консалтинговые компании, на договорных началах является выгодным, поскольку помогает предприятию в кратчайшие сроки получить необходимую информацию, не создавая внутренние информационные структуры. Полученная информация позволит руководителю предприятия принимать экономически обоснованные решения по управлению процессом в условиях ограниченности ресурсов. Как стратегический ресурс информация является основой для маневра, позволяет отслеживать и прогнозировать изменения (накапливаемые и происходящие во внутренней и внешней средах предприятия в процессе реализации инноваций), оценивать возможности инноваций, а также значительно снижать риск и неопределенность в процессе принятии решений.

В настоящее время информационная поддержка инновационной деятельности переходит на качественно новый уровень, создаются базы данных национальных программ научно-технических разработок и инновационных программ, соответствующие формату данных и формам доступа мировых информационных сетей. Но существующие системы информационного обеспечения инновационных процессов на отечественных предприятиях пока еще остаются недостаточно развитыми, а попытки их расширять требуют коренных институционных реформ.

Предприятие может повысить эффективность информационного обеспечения управления информационными процессами за счет превышения скорости обобщения и систематизации информации над скоростью реализации инноваций, что достигается не столько за счет улучшения механизмов обмена информацией между участниками инновационных процессов, сколько улучшения методов преобразования информации в знания или интеллектуальный капитал предприятия.

Не менее важным для повышения качества информационного обеспечения инноваций на российских предприятиях является улучшение национальной информационной инфраструктура инновационной деятельности в целом.

Главные направления развития национальной информационной инфраструктуры научно-инновационной сферы включают в себя:

- развитие национальной информационной инфраструктуры и информационных ресурсов (информационное обеспечение различных стадии инновационного процесса);
- развитие высокопроизводительных вычислительных ресурсов (инструмент для разработки и развития высокотехнологичных и наукоемких инновационных проектов);
- развитие компьютерных сетей (предоставление участникам инновационного процесса соответствующего доступа к структурированным информационным ресурсам, а также обеспечение взаимодействие участников этого процесса);
- разработка и использование современных и эффективных информационных технологий (ускорение таких процессов как: процесс проектирования наукоемкой техники, высокоэффективных технологических процессов).

Подводя итоги, следует отметить, что эффективность современной экономики во многом зависит от уровня развития информационного обеспечения, которое позволяет получить доступ

к необходимой информации в короткие сроки. Кроме того, с формированием инновационной экономики роль информационной составляющей только усиливается. Это связано с тем, что процессы формирования инновационной экономики требуют комплексного решения технических, технологических, социально-экономических проблем в отраслях и на предприятиях. Данные проблемы требуют системного комплексного информационного обеспечения. Однако существующие системы информационного обеспечения инновационных процессов на отечественных предприятиях пока еще остаются недостаточно развитыми и нуждаются в значительных структурных реформах, для которых требуются денежные вложения.

УДК 004:658.5

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

МОДЕЛИРОВАНИЕ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Инвестиционная деятельность является необходимой составляющей хозяйственной деятельности современного предприятия. Основная сущность этой деятельности заключается в целевом формировании и распоряжении своими или заемными средствами финансовых ресурсов.

Залогом успешной инвестиционной деятельности принято считать правильно сформированную инвестиционную политику. Инвестиционная деятельность, как правило, осуществляется предприятием с целью обеспечения максимального благосостояния его собственников в нынешнем и будущем периодах, что в конечном итоге выражается в увеличении рыночной стоимости предприятия.

Целью управления инвестиционной деятельностью выступает определение перспективных объектов инвестирования, поиск, необходимых для этого инвестиционных ресурсов, разработка инвестиционной программы и мероприятий по ее реализации.

Сложность управления инвестиционной деятельностью объясняется тем, что сама эта деятельность – процесс комплексный и динамичный, требующий управленческих решений, связанных между собою и не противоречащих друг другу. Последнее является гарантией эффективности инвестиционной деятельности.

Традиционно процесс инвестиционной деятельности описывается с точки зрения 3-х стадий: прединвестиционной, инвестиционной, постинвестиционной. Сосредоточим свое внимание на прединвестиционной стадии, более тщательно детализируя ее.

Так, эта стадия включает в себя следующие этапы: 1) рассмотрение потенциала предприятия; 2) создание инвестиционной политики и стратегическое планирование реализации инновационного проекта; 3) реализация и оценка соответствия инвестиционной политики и стратегии критериям оптимальности.

Визуализация перечисленных этапов дает возможность инвестиционному менеджеру, имеющему незначительный опыт, более наглядно представить масштаб и направления этой деятельности. Средства визуализации разнообразны, но нами был сделан выбор в пользу программы Enterprise Architect. При помощи инструментов этой программы была создана диаграмма активностей, на которой были выделены основные объекты моделирования, в основу которых легли выше перечисленные этапы инвестиционной деятельности предприятия.

Первый этап инвестиционной деятельности «Рассмотрение потенциала предприятия» (см. рис. 1) сопряжен с анализом эффективности хозяйственной деятельности предприятия, поскольку он дает представление о его существующем потенциале.

Заключение о существующем потенциале предприятия предопределяете плановые горизонты этого предприятия, а именно, - инвестиционную политику и инвестиционную стратегию, отличающиеся своей длительностью применения, а также целостностью и гибкостью. Одной функцией планирования на этом этапе не ограничиваются, так как необходимо предусмотреть определенные направления и механизмы внедрения (рис. 2).

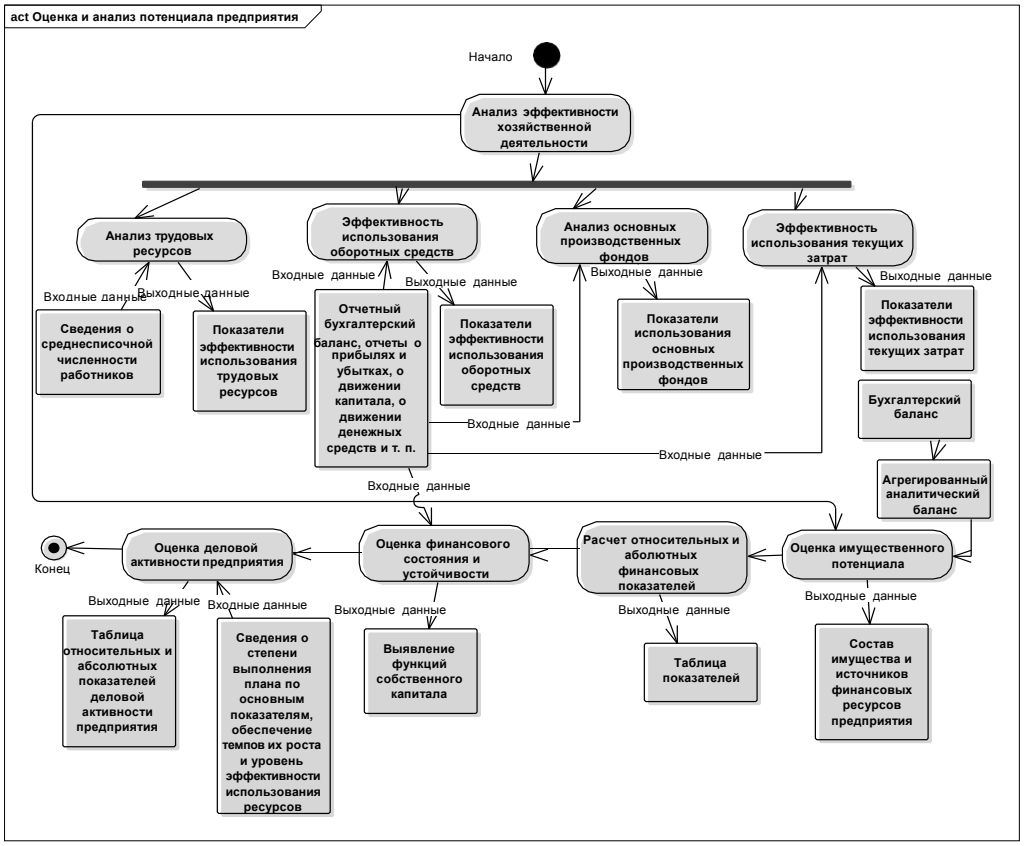


Рис. 1. Декомпозиция этапа «Рассмотрение потенциала предприятия»

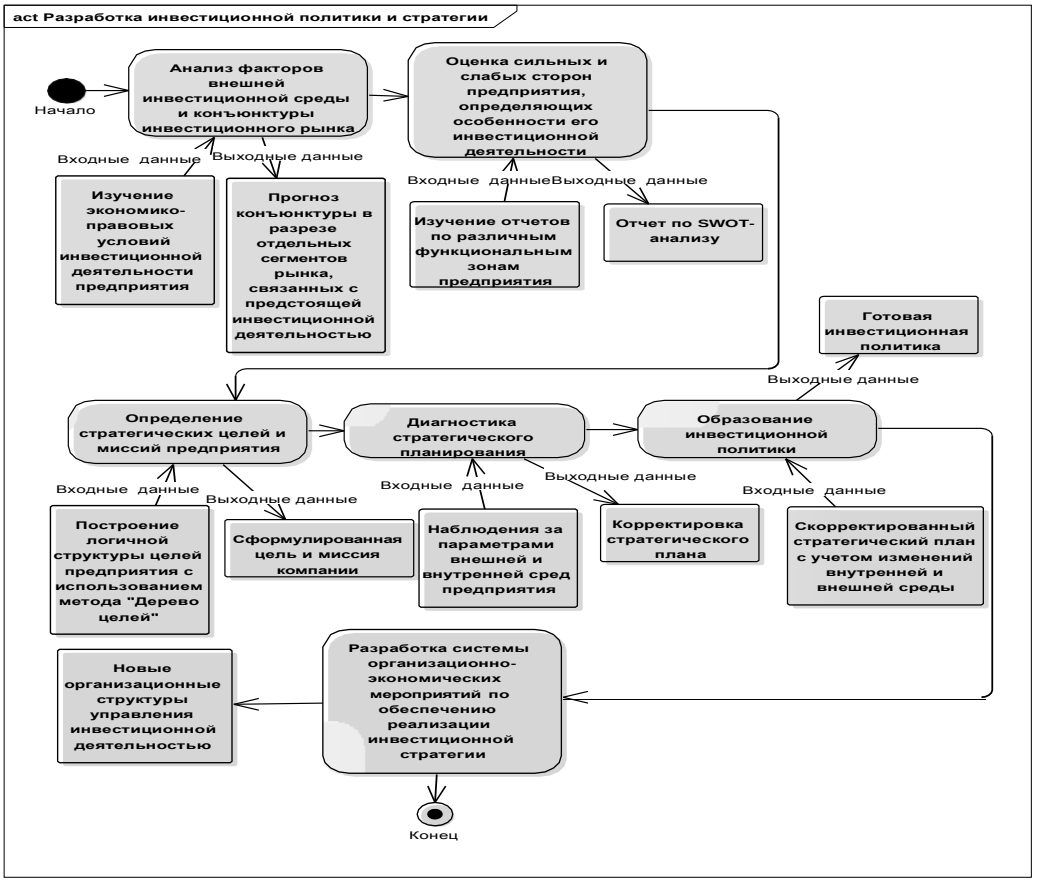


Рис. 2. Декомпозиция этапа «Создание инвестиционной политики и стратегическое планирование реализации инновационного проекта»

Заключительный этап инвестиционной деятельности, смоделированный в виде рисунка 3, дает осознание того, правильно ли был сделан выбор инвестиционного проекта с точки зрения его затрат, эффективности, окупаемости и рисков. Этот этап приобретает особую важность, если речь идет о выборе нескольких инвестиционных проектах. Именно на этом этапе поднимается вопрос о безопасности вложения средств, как самого предприятия, так и внешнего инвестора.

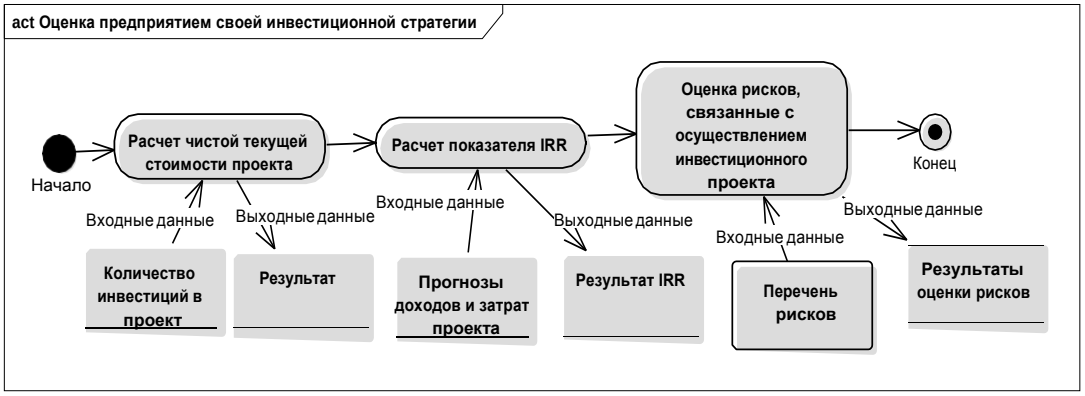


Рис. 3. Декомпозиция этапа «Реализация и оценка соответствия инвестиционной политики и стратегии критериям оптимальности»

Таким образом, моделируя инвестиционную деятельность предприятия, необходимо определить:

- сущность и характеристики деятельности;
- стадии деятельности;
- этапы деятельности и содержание этих этапов;
- средство моделирования (методологию, программное средство и т.д.).

Обеспечивая информационную безопасность предприятия на каждом из декомпозированных этапов прединвестиционной стадии, важно определить индикаторы этой безопасности. Например, на этапе «Рассмотрение потенциала предприятия» внимание приковано к финансово-экономическим показателям предприятия, которые составляют его коммерческую тайну. Все здесь зависит от организационно-правовой формы предприятия. Предприятия, относящиеся к корпоративному сектору, обязаны гарантировать прозрачность своей документации и, следовательно, показателей.

К информации, представляющей коммерческий интерес и генерируемой на этапе «Создание инвестиционной политики и стратегическое планирование реализации инновационного проекта», относят направления, мероприятия, источники, объемы инвестирования и др. Обеспечение защиты и рациональное использование именно такой информации возможно при условии тщательного и критического отбора ее пользователей, а также определение четких правил доступа к ней.

Этап «Реализация и оценка соответствия инвестиционной политики и стратегии критериям оптимальности» характеризуется наличием информации о целесообразности инвестирования, т.е., о намерениях предприятия, которые в условиях конкурентной борьбы не всегда имеет смысл разглашать. В то же время, для стороннего инвестора эта информация должна быть доступна.

Подводя итог сказанному, отметим, что информационная безопасность предприятия зависит от многих аспектов, среди которых способы и источники инвестирования, форма функционирования предприятия, условия доступа к информации и др.

УДК 659:005

Герасимова Светлана Васильевна
д.э.н., профессор
Дегтерева Ксения Сергеевна
студентка 4-го курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ О ВНУТРЕННЕЙ ИНВЕСТИЦИОННОЙ СРЕДЕ ПРЕДПРИЯТИЯ

Введение. В период динамичных перемен очевидна необходимость предварительного анализа как внешней, так и внутренней среды предприятия. Это, во-первых, обусловлено тем, что принятие управленческого решения на основе, полученной в ходе анализа информации, является залогом его эффективности, во-вторых, результаты анализа могут быть полезны не только для использования в перспективе, но, и применены для укрепления уже существующего потенциала, например, для обеспечения информационной безопасности. Возможности, получаемые в результате анализа, особенно актуальны для предприятия, активно осуществляющего инвестиционную деятельность, поскольку инвестиционный анализ способствует и исправлению ошибок, что важно в современных условиях хозяйствования.

Топ-менеджмент большинства предприятий уже не отрицает значимость эффективного плана управления инвестициями, так как четкое распределение денежных потоков гарантирует достижение целей этого предприятия. Также общеизвестно, что основой любого плана являются результаты, проведенного ранее анализа инвестиционной среды предприятия. И, если на внешнюю среду предприятие влиять не в силах, то внутренняя среда, порой представляющая коммерческую тайну для аутсайдеров, является одним из объектов управления этого предприятия.

Цель и задачи исследований. Целью исследования является определение сущностных характеристик инвестиционной среды предприятия. Задачами исследования выступают: 1) конкретизация понятия «инвестиционная среда»; 2) уточнение составляющих элементов инвестиционной среды; 3) выделение мероприятий по целесообразному использованию информации о состоянии внутренней инвестиционной среды.

Изложение результатов. Исследование сущности инвестиционной среды как понятия указали на встречающиеся отождествления его с другими понятиями, например, таким как инвестиционный климат. Обобщив существующие научные подходы, констатируем, что инвестиционная среда – это как благоприятные, так и не благоприятные условия для осуществления инвестиционной деятельности в стране, в регионе, в отрасли, на предприятии.

Различают внутреннюю и внешнюю среду предприятия. В общем понимании внешняя среда, как правило, представляет собою совокупность экономических, демографических, социально-культурных, политико-правовых, научно-технических, природно-географических и других факторов. Как было уже отмечено выше, внешняя среда не поддается контролю и влиянию со стороны предприятия, ее можно только анализировать и оценивать. Внутренняя среда предприятия также подвергается оценке и анализу, в результате чего возможно ее дальнейшее изменение усилиями предприятия. Свои усилия предприятие, прежде всего, направляет на собственный персонал, потенциальных потребителей, партнеров по бизнесу, конкурентов и др. Перечисленное и является составляющими внутренней среды предприятия.

Сосредотачиваясь на инвестиционном аспекте, охарактеризуем внутреннюю инвестиционную среду предприятия, которая представлена субъектами, объектами, принципами, потребностями и др. К субъектам инвестиционной среды предприятия отнесем финансовых менеджеров, которые должны обладать соответствующим опытом, навыками, умениями и стремлениями. Объектами инвестиционной среды могут выступать конкурентоспособность, рентабельность, финансовая устойчивость и прочие показатели предприятия. Это и есть те факторы, которые могут обусловить определенный инвестиционный интерес и позволить выявить сильные и слабые стороны предприятия. Существенное влияние во внутренней инвестиционной среде предприятия играют и такие факторы как инвестиционные принципы, приоритеты, потребности. С учетом этих факторов становится возможным определение масштаба, объема, направлений инвестиционной деятельности.

Выделенные характеристики внутренней инвестиционной среды предприятия предопределяют ее некую секретность. Безусловно, если речь идет о внешнем инвесторе, то

должна быть обеспечена достаточная «прозрачность» показателей предприятия. В случае инвестирования за счет собственных ресурсов, предприятие должно позаботиться об информационной безопасности относительно своих инвестиционных возможностей. Поэтому понятно, по каким причинам понятие «инвестиционная среда» по смыслу иногда отождествляется с понятием «инвестиционный потенциал».

Речь не идет о сокрытии или искажении данных об истинном состоянии внутренней инвестиционной среды предприятия, а только об умелом и грамотном их использовании на благо предприятия. В связи с этим, целесообразно выделить источники информации. К ним отнесем планы, концепции, стратегии, из которых можно узнать о приоритетах, направлениях и масштабах инвестиционной деятельности предприятия. Разные показатели предприятия, как правило, декларируются в отчетах, заключениях, прогнозах. Как известно, отчетность может быть обязательной, а значит доступной для определенного круга пользователей, и может быть отчетность только для внутреннего использования.

Защита перечисленных информационных источников со стороны предприятия может быть обеспечена при помощи таких мероприятий:

1) разработка и принятие корпоративного кодекса, который бы обязывал персонал предприятия соблюдать коммерческую тайну предприятия и предусматривал административные воздействия в случае ее не соблюдения;
2) надежная техническая защита информации, находящейся в электронной форме, при помощи компьютерных программ и приложений;
3) четкое определение перечня генераторов и пользователей отчетности и прочей информации;
4) тщательный контроль движения и размещения информации, предназначенной как для узкого, так и широкого пользования.

Выводы. Инвестиционная среда предприятия является одним из объектов анализа, который анализируется непрерывно. Результаты такого анализа используются для выбора типа инвестиционной политики предприятия, а впоследствии – для разработки его инвестиционной стратегии. Инвестиционная среда предприятия предполагает собою набор условий, способствующих или не способствующих, а также не достаточно способствующих осуществлению эффективной инвестиционной деятельности предприятия. Инвестиционная среда формируется как внутри самого предприятия, так и за его пределами, образовывая тем самым внешнюю и внутреннюю среды. Анализ каждой из сред является важным для предприятия, но с точки зрения управления и влияния со стороны предприятия в больше мере отмечается его внутренняя инвестиционная среда. Возможность влияния предприятия на формирование своей внутренней инвестиционной среды должна им использоваться и в целях обеспечения собственной информационной безопасности.

УДК 303.722.29

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

ФАКТОРЫ, ВЛИЯЮЩИЕ НА БЕЗОПАСНОСТЬ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Предприятие как хозяйствующий субъект должно осуществлять три основных вида деятельности – финансовую, операционную и инвестиционную, которые формируют уровень его безопасности. Финансовая деятельность сопряжена с движением денежных средств, организацией денежных потоков, генерируемых как на основе собственного, так и заемного, а также привлеченного капитала. Кроме этого, финансовая деятельность предприятия предусматривает изменение размеров и структуры капитала. Операционная деятельность предприятия направлена на производство и продажу товаров и услуг. Основной целью инвестиционной деятельности предприятия является вложение средств, предполагающее дальнейшее увеличение их объема. Инвестиционная деятельность предприятия многогранна, требует особой политики управления, следовательно, подлежит более тщательному

теоретическому анализу.

Изучение современных научных источников позволило сформировать мнение, что наиболее распространенной проблемой, связанной с осуществлением инвестиционной деятельности предприятием, является проблема ее низкой эффективности. Также изучение источников или причин возникновения этой проблемы указало на факторы, которые изначально формируют определенный уровень эффективности. Сделанные выводы сориентировали данное научное исследование в сторону идентификации факторов, наиболее всего влияющих на инвестиционную деятельность предприятия, их систематизация и конкретизация степени воздействия на объемы инвестирования.

Методом и инструментом комплексного и системного исследования выступил факторный анализ, результатом которого должны стать качественные и количественные оценки факторов. Дадим краткую качественную характеристику факторам, предопределяющим эффективность инвестиционной деятельности предприятия.

Так, в учебных изданиях чаще всего описываю две группы факторов:

1. Субъективные (зависящие от деятельности предприятия) и объективные (не зависящие от деятельности предприятия) факторы.
2. Макроэкономические (характеризующие инвестиционную среду на уровне государства, региона, отрасли) и микроэкономические (характеризующие инвестиционную среду предприятия) факторы.

Влияние субъективных факторов контролировать и оценивать легче всего, так как к ним традиционно относят политику и качество управления на предприятии, определенные предприятием приоритеты и ориентиры, свобода выбора направлений развития и др.

Объективные факторы, возникающие, как правило, во внешней среде предприятия (стихии, кризисы), могут быть только отслежены и не всегда на ранней стадии. Предприятие практически не в силах предотвратить их воздействие на свою инвестиционную деятельность, возможно только уменьшение этого воздействия.

Макроэкономические факторы могут воздействовать на предприятие одновременно, с разной силой и с разных позиций, а именно - экономической, правовой, социальной, политической и административной. Например, с точки зрения экономической позиции на предприятие могут оказывать воздействие такие факторы как темпы роста производства, инфляция, занятость, ценообразование, доступность кредитов и др. Правовое влияние на предприятие осуществляется через соответствующую законодательную базу с учетом ее степени жесткости. Также не стоит забывать о социальной обстановке и уровне качества жизни граждан, а именно пенсионный возраст, уровень пенсий и др. Влияние факторов политической окраски тесно связано с межгосударственными отношениями, что, в свою очередь, сказывается на объемах иностранного инвестирования, на привлекательности российских предприятий для иностранных инвесторов. По-прежнему актуальны и сильны административные воздействия на предприятие со стороны чиновников, имеющих отношение к реализации инвестиционных проектов. Общеизвестно, что это воздействие может проявляться либо в одобрении, либо в отказе в содействии.

На микроуровне формируются уже совершенно другие, но контролируемые со стороны предприятия, факторы. Это, прежде всего, конкурентоспособность выпускаемой продукции либо услуги, перспективы развития фирмы, поддержание марки организации, степень износа основных фондов производства и многое другое.

Как было уже отмечено выше, факторы можно идентифицировать как контролируемые и неконтролируемые. Считаем, что субъективные факторы и факторы микро-уровня – контролируемые. Объективные факторы и факторы макро-уровня – не контролируемые. Кроме того, каждый фактор имеет свою степень влияния в зависимости от выбранного направления инвестиционной деятельности предприятия. В концептуальном смысле общими вариантами воздействия перечисленных групп факторов на эффективность инвестиционной деятельности предприятия могут быть – стимулирование, торможение, отсутствие возможности ее осуществления.

Например, уменьшение фактического объема валового внутреннего продукта свидетельствует о негативных тенденциях, сложившихся в промышленной сфере. К таким тенденциям можно отнести потерю рынков, снижение конкурентоспособности страны и т.д. Следуя производственной цепочке, для предприятия это чревато отсутствием спроса на продукцию, разладом партнерских отношений, потерей прибыли, снижением финансовой устойчивости и др. В таких ситуациях инвестиционная деятельность представляет для предприятия наименьший интерес, разве только с целью спасения его от банкротства. Но здесь

также наблюдается масса негативных последствий, среди которых наиболее распространенным в наше время является внешнее управление предприятием.

Следующий пример, связан с влиянием такого макроэкономического фактора как инфляция, высокий уровень которой уменьшает инвестиционные возможности предприятия по причине снижения амортизационных отчислений, формирующих фонд его собственных инвестиционных ресурсов, а также по причине увеличения реальной ставки налогообложения прибыли. Все перечисленное не является единственным негативным последствием для предприятия. Так, инфляция учитывается и при определении уровня заработных плат его работников. Увеличение фонда заработной платы вынудит предприятие увеличить оборотные фонды, что происходит чаще всего за счет собственных резервов, которые при более благоприятных условиях могли бы быть направлены на инвестиционные нужды.

Таким образом, можно констатировать, что наибольшей степенью воздействия на эффективность инвестиционной деятельности предприятия обладают объективные факторы и факторы макро-уровня, потому что характеризуются как неконтролируемые. С точки зрения возможных негативных последствий или создания угроз, они могут быть идентифицированы как наиболее опасные для предприятия. В тоже время, степень опасности можно уменьшить при помощи постоянного наблюдения за изменениями, обусловленными этими факторами, и проведением мероприятий предупреждающего характера. Поскольку влияние факторов может быть не только отрицательным, но и положительным, декларируем мысль о существовании устойчивой зависимости между изученными нами факторами и безопасностью предприятия, в нашем случае, финансовой безопасностью

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Маслов Александр Витальевич
магистрант
Таврическая академия
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ОСНОВЫ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В наше время информационная безопасность является неотъемлемой частью любого предприятия нашей страны. Информационная безопасность предполагает собой защиту интеллектуальной собственности организации, а также предотвращает попытки несанкционированного доступа к ней.

Защита информации включает полный комплекс мер по обеспечении целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права. В свою очередь для пользователей должна быть создана инструкция, которая регулирует правила использования корпоративной сети.

Система информационной безопасности состоит из четырех подразделений:

1. Компьютерная безопасность. Работа этого подразделения основана на принятии технологических и административных мер, которые обеспечивают качественную работу всех аппаратных компьютерных систем, что позволяет создать единый, целостный, доступный и конфиденциальный ресурс.
2. Безопасность данных - это защита информации от халатных, случайных, неавторизированных или умышленных разглашений данных или взлома системы.
3. Безопасное программное обеспечение - это целый комплекс прикладных и общецелевых программных средств, направленных на обеспечение безопасной работы всех систем и безопасную обработку данных.
4. Безопасность коммуникаций обеспечивается за счет аутентификации систем телекоммуникаций, предотвращающих доступность информации неавторизированным лицам, которая может быть выдана на телекоммуникационный запрос.

Таким образом для обеспечения информационной безопасности система должна быть предельно проста для технического обслуживания и доступна для пользователей. Пользователей следует максимально ограничить в доступе к информации, которая им не нужна для выполнения своих обязанностей. Обязательно необходимо предусмотреть автоматическое включение и выключение всей системы в случае экстремальных ситуаций.

УДК 621

Деркач Юлия Владимировна
главный специалист
по кадровому делопроизводству, к. пед. н.
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Акинина Людмила Николаевна
старший преподаватель
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ

Одним из приоритетных направлений научных исследований в области информационной безопасности Российской Федерации являются вопросы развития и совершенствования системы подготовки кадров, работающих в сфере обеспечения информационной безопасности, поскольку без создания специальных служб защиты, укомплектованных высококвалифицированными кадрами, невозможно эффективное развитие любого региона.

Вопросы подготовки кадров по информационной безопасности в России получили развитие с 1992 г., когда была сформирована межвузовская научно-техническая программа «Методы и технические средства обеспечения безопасности информации».

В период между 1992 и 1998 гг. сложился крупный коллектив исполнителей, в состав которого вошли 15 крупнейших вузов России, главным среди которых стал Московский инженерно-физический институт (МИФИ).

В настоящее время специализированную подготовку в области безопасности на российском рынке информационных технологий обеспечивают как учебные центры, для которых это направление является приоритетным, так и учебные центры, специализирующиеся на обучении по всему спектру проблем в сфере информационных технологий и телекоммуникаций. Тематику обучения составляют как авторизованные зарубежные курсы международных центров обучения по защите информации, так и авторские курсы отечественных учебных центров, разработанные с учетом специфики российского рынка.

Основные направления многоуровневой системы подготовки кадров в области информационной безопасности представлены в таблице 1.

Таблица 1.

Система подготовки кадров в области информационной безопасности

Уровень подготовки	**Срок обучения**
подготовка молодых специалистов на базе школьного образования	5-5,5 лет
подготовка специалистов на базе среднетехнического образования через колледж на базе 9 классов	4-5 лет
подготовка специалистов по информационной безопасности на базе высшего технического образования	2-2,5 года
подготовка специалистов высшей квалификации через аспирантуру и защиту диссертационных работ в специализированных советах	2-2,5 года
переподготовка кадров на краткосрочных курсах повышения квалификации специалистов и руководителей подразделений	2-4 недели

К базовым условиям, обеспечивающим качественную подготовку специалистов в области защиты информации, относят:

- взаимосвязь учебного процесса с научными исследованиями в области информационной безопасности;
- материально-техническое обеспечение учебного процесса;
- обеспечение учебного процесса педагогическими кадрами высшей квалификации.

УДК 004:005.9

Землячев Сергей Викторович
к.э.н., доцент кафедры финансов предприятий и страхования
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАТИЗАЦИЯ КОММУНИКАЦИЙ СТРАХОВЩИКА

Под коммуникациями страховщика понимаются все «сигналы», которые он направляет своим страхователям, потенциальным клиентам, своим сбытовым сетям, общественному мнению и т.д. Коммуникации страховщика обеспечивают практическую реализацию маркетинговых исследований, проведенных на стадии анализа рынка и разработки страховой продукции. На этапе коммуникаций реализуются итоги сегментации и поиска наиболее предпочтительных потребительских групп, выбор аргументов воздействия на клиентов, положительные свойства страхового продукта. Итога коммуникаций подтверждают правильность или показывают ошибочность маркетинговой стратегии страховщика. По сути, коммуникации – это основная часть оперативного маркетинга страховщика, представляющего реальные практические действия на рынке. Оперативный маркетинг входит наряду с исследованиями рынка и оптимизацией внутренней среды компании (организационным маркетингом) в единый комплекс страхового маркетинга.

Различают внутренние и внешние коммуникации. Внутренние коммуникации рассчитаны на создание прозрачной внутренней среды страховой компании, тогда как внешние коммуникации рассчитаны на общественное мнение, страхователей и потенциальных потребителей страховой продукции.

По мере ужесточения конкуренции, развития общественного мнения и движения в защиту прав потребителей российские страховые компании должны уделять все больше внимания своим внутренним и внешним коммуникациям. На уровне страховой компании должна существовать единая стратегия коммуникаций, объединяющая и интегрирующая все усилия на этом направлении.

Стратегия коммуникаций должна объединять в себе все внешние связи страховщика (взаимодействие первых лиц компании с партнерами; общение с представителями СМИ и др.) и внутренние коммуникации компании со своими подразделениями.

Цель единой стратегии коммуникаций – это достижение наилучшего коммерческого результата страховой компании при минимизации вложений в организацию и контроль ее деятельности. Коммуникации способствуют улучшению экономического результата за счет преодоления разрозненности и замкнутости структурных подразделений страховой компании, за счет налаживания контактов страховщика с клиентами, внедрения его торговой марки и услуг в повседневную жизнь потребителей.

Стратегия коммуникаций страховщика включает следующие составляющие:

-создание системы идентификации компании среди конкурентов (работа, направленная на повышение известности своей торговой марки среди населения, создание единого звукового, графического, цветового и образного рядов, ассоциирующихся у клиента со страховой компанией); совершенствование коммуникаций при продаже страховой продукции (агентская деятельность, реклама конкретной страховой продукции и т.д.);

-создание благоприятного социально-психологического климата среди сотрудников страховой компании, ее партнеров, а также фиделизированной клиентуры;

-система анализа эффективности коммуникаций.

Внутренние коммуникации необходимы, чтобы связать воедино комплекс отдельных подразделений страховой компании, создавая единую систему корпоративных ценностей, традиций и интересов. Цель внутренних коммуникаций – достижение такого положения, при котором каждый сотрудник страховой компании гордился бы принадлежностью к ней, старался в максимальной степени оправдать доверие корпорации.

Внешние коммуникации направлены на: ознакомление потенциальных потребителей со страхованием и со своими страховыми продуктами; продвижение на рынок или его целевые сегменты страховых продуктов страховщика; улучшение имиджа страховщика в общественном сознании. Главное их назначение – увеличение объема продаж страховой продукции.

Оптимальная стратегия коммуникаций должна быть в наибольшей степени приспособлена к потребностям каждой конкретной страховой компании – особенностям технологического процесса и свойствам клиентуры. Стратегия коммуникаций страховщика должна также

строиться с учетом достижения максимального эффекта на каждый рубль затрат на осуществление коммуникаций.

При этом в системе внешних коммуникаций недостаточно внимания уделяется процессу информатизации. Важным является организации информационной системы и ее процессов с использованием: бизнес-правил учета страховой информации, структуры и логики базы данных страховой информации, классификации элементов учета, правил создания технологичных с точки зрения автоматизации страховых продуктов.

Результатами внедрения информационной системы для страховой компании будут выступать: качественно новый уровень менеджмента; оптимизация и документирование всех учетных процессов; количественная и качественная оценка всех учетных задач; экономия времени и расходов на ведение дела; максимальная детализация учитываемых данных; использование методов страховой математики и статистики; реализация эффективных технологий обслуживания клиентов; учет сложных страховых продуктов, работа в глобальных сетях.

Одним из главных вопросов, которые необходимо решить в сфере финансовой устойчивости страховых компаний, является строгое согласование страховой премии с риском. Необходим переход к точной, научно разработанной системе вероятностей. Только путем четкого определения всех учетных показателей и эффективной обработки информации можно обеспечить стабильное гарантированное качество предоставления услуг. Это целесообразно также отнести к задачам, которые решает информационная система. Технологически данная система должна обеспечить процесс коммуникаций следующими процессами: учет всех выданных полисов; отражение каждого поступления платежа в бухгалтерском учете; централизованный в рамках компании учет всех клиентов и застрахованных объектов; учет всего процесса урегулирования убытков; учет информации в размере страховых рисков; возможность работы территориально удаленных офисов с общей базой данных.

Работа данной системы будет являться составляющей информационного обеспечения менеджмента страховой компании, так как позволит сопровождать:

-менеджмент клиентов (информация по каждому клиенту и по группам клиентов; мониторинг взаимодействий с клиентом);

-менеджмент объектов (ведение полной страховой информации по каждому застрахованному объекту и по группам объектов);

-менеджмент договоров (по страхованию, перестрахованию, сострахованию: автоматическое приостановление действия, аннулирование и возобновление действия договора, передача рисков в перестрахование);

-менеджмент комиссионных вознаграждение посредникам;

-менеджмент урегулирования убытков (прием заявок, учет претензий, описания пострадавших объектов, связь с перестрахованием и др.);

-анализ информации по структурным подразделениям компании;

-предоставление данных управленческого учета для руководства страховщика.

УДК 004:005.9

Землячева Ольга Андреевна
ассистент кафедры финансов предприятий и страхования
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ В ФИНАНСОВОМ И СТРАХОВОМ МЕНЕДЖМЕНТЕ

Информация играет исключительно важную роль в корпоративном управлении. Только на основе внешней и внутренней информации возможно правильное позиционирование предприятия в окружающей среде и постановка стратегических целей. Реализация стратегии предусматривает детализацию целей, уточнение планов и бюджетов. Затем на основе учетных данных осуществляется план-факторный анализ, позволяющий оценить успешность выполнения стратегических планов.

Информационное обеспечение финансового менеджмента заключается в подготовке, нахождении и использовании общеэкономической, бухгалтерской, финансовой, коммерческой, статистический, экспертной и другой информации. Важным источником информации для

управления финансами на предприятии является обязательная бухгалтерская и налоговая отчетность, а инструментом для ее использования – обеспечение менеджмента электронными средствами коммуникаций. Для крупных предприятий и организаций информационное обеспечение управления – одна из наиболее острых, а иногда и критических проблем, поэтому необходимо постоянное повышение квалификации финансовых менеджеров. В настоящее время система бухгалтерского и налогового учета автоматизируется. Но, несмотря на очевидные преимущества, перевод бумажных документов в электронную форму – сложная проблема. Для крупных предприятий это связано с огромным потоком документов, для мелких – с их ограниченными финансовыми возможностями, недостатком квалифицированных кадров и т.п.

Вопросы информационной поддержки финансового менеджмента должны рассматриваться в неразрывной связи с вопросами информационной поддержки корпоративного управления в целом. Необходима единая интегрированная система информационного обеспечения. Информационно-управляющая система – это формальная структура сбора, обработки и передачи данных для выдачи руководству информации, необходимой для принятия решений. Общей целью информационной системы является облегчение эффективного выполнения функций планирования, контроля за производственной деятельностью, а самой важной ее задачей – выдача нужной информации нужным людям и в нужное время.

Необходимость обработки информации с целью ее анализа, обобщения и представления в удобной для анализа форме возникла давно, и также давно были найдены соответствующие формы, например, бухгалтерский анализ, журнал учета поступлений и выплат, различные статистические отчеты. Увеличение объемов деятельности, различных форм обязательной отчетности, объема вычислительных операций в условиях постоянно растущих затрат на содержание квалифицированного персонала вызвали потребность в автоматизации процесса обработки и распределения информации. В идеале автоматизированная информационно-управленческая система должна обеспечивать возможность обработки и получения информации в необходимой форме в реальном масштабе времени, т.е. практически сразу после появления первичной информации о каком-либо событии. Автоматизация позволяет повысить качество информации, а именно: ее точность, достоверность, актуальность, полезность и полноту отражения всей совокупности значимых фактов.

Особую проблему в решении вопросов информационного обеспечения управления страховым бизнесом представляет получение информации о внешней среде. Внешняя среда компании включает экономические условия, потребителей, правительственные акты, законодательство, конкурирующие организации, систему ценностей в обществе, профессиональные общественные организации, технику и технологию, другие составляющие. Эти взаимосвязанные факторы оказывают влияние на все, что происходит внутри страховой компании. Большое значение имеет и тот факт, что, хотя компания и зависит полностью от внешней среды, эта среда, как правило, находится вне пределов влияния самой компании.

С каждым годом приходится учитывать все большее количество факторов внешней среды, и процесс этот принимает поистине глобальный характер. Выделяют две основные группы факторов – прямого и косвенного воздействия.

К факторам прямого действия относятся факторы, которые непосредственно влияют на операции компании и могут испытывать на себе, в свою очередь, влияние проводимых ею операций. Применительно к страховщикам такими факторами являются:

-нормативная среда, т.е. законодательные и нормативные акты о страховании;

-состояние (конъюнктура) страхового рынка на территории, где действует компания (платежеспособность клиентов, их потребность в различных видах страхования, конкурентная среда и др.);

-географическое положение территории (природно-климатическая зона, наличие границ с другими государствами, население, наличие и вид коммуникаций и т.д.);

-социально-экономическое положение территории (вид и уровень развития промышленности, сельского хозяйства, экономические связи и формы этих связей с другими территориями, уровень жизни и занятость населения);

-состояние территориального финансового рынка (качественный состав действующих банковских и финансовых учреждений, инвестиционная политика и инвестиционные инструменты и т.п.);

-состояние территориального рынка труда (наличие специалистов, оплата труда, затраты на обучение и переподготовку).

В отличие от предприятий промышленности и сферы нестраховых услуг страховщики в большей степени зависят от природной и социально-экономической среды. Это объясняется

влиянием природных и техногенных факторов на вероятность возникновения страховых случаев и, следовательно, на объем выплат и финансовые результаты деятельности, а также отсутствием повсеместного устойчивого спроса на страховые услуги и, как следствие, зависимостью спроса от территориальных особенностей размещения промышленности, транспортных узлов и терминалов, а также уровня жизни населения.

К факторам непрямого или косвенного воздействия следует отнести факторы, которые могут не оказывать прямого немедленного воздействия на результаты работы компании, но, тем не менее, сказываются на них: общее состояние экономики, научно-технической прогресс, социокультурные и политические изменения, влияние групповых интересов и существенные для бизнеса события в других странах. На развивающийся страховой рынок в наибольшей степени косвенное воздействие оказывает состояние экономики и групповые интересы в отраслях отечественной промышленности.

Таким образом, основные требования к интегрированным информационным системам: вся информация находится в общей информационной среде, доступна сотрудникам независимо от нахождения, доступ определяется только правами, максимальный срок получения информации регламентирован. При внедрении интегрированной информационной системы необходима современная методология, позволяющая внедрять информационную систему в срок, в рамках выделенных ресурсов с запланированной функциональностью, с ответственностью за конечный результат.

Внедрение информационной системы позволяет переходить на новые методы управления, на качественно новый уровень менеджмента и предоставления страховых услуг.

УДК: 32.019.51

Korshunova Irina Grigorievna
Senior teacher
Krasnodar University of Interior, Crimean Affiliate
Daraiskyi Vialyi
Cadet of the Krasnodar University of Interior, Crimean Affiliate

IT SECURITY PROBLEMS AND LEGAL PROVISION INFORMATION SECURITY IN THE RF

In the modern global world network safety has crucial importance. The entities need to provide safe access for employees to network resources at any time. That is why the modern strategy of providing network safety must consider a number of such factors as increase in reliability of network, effective management of safety and protection against constantly evolving threats and new methods of the attacks. For many companies the problem of ensuring network safety becomes harder and harder since today's mobile employees using personal smart phones, laptops and tablets for work introduce new potential problems. At the same time, hackers aren't idle too and their new cyber threats are more and more sophisticated.

Recent poll of the IT specialists managing network safety (the carried-out by Slashdotmedia) showed that among important factors concerning choice of network solutions of safety nearly a half of respondents on the first place put reliability of the chosen network decision.

The vulnerabilities connected with network safety leave open a number of potential problems and put the company at various risks. IT system can be compromised through them, information can be stolen, workers and clients can receive problems with access to resources which they are authorized to use that can force customers to pass to the competitor.

You can have the service idle time connected with problems with safety and other financial consequences. For example, the website, idle in rush hour, can generate both direct losses, and powerful negative PR that will obviously affect sales level in the future. Besides, in some industries there are strict criteria on resource availability which violation can lead to regulatory penalties and other unpleasant consequences.

In addition to reliability of decisions, there is still a number of the questions which came today to the forefront. For example, about 23% of the interviewed IT specialists allocate the cost of the decisions as one of the main problems connected with network safety. It isn't surprising, considering that IT budgets of the last several years were significantly limited. Further, about 20% of respondents marked out simplicity of integration as priority parameter in case of the choice of the decision. What is natural in conditions when demand from an IT of department is carried out by small resources.

About 9% of respondents called network functions as a key factor in case of the choice of decisions in the field of network safety. In case of the choice of the decision on ensuring network safety of corporate systems and minimization of the risks connected with it, one of the major factors for nearly a half (about 48%) of respondents, there was reliability of network and the related decision.

Today hackers use various methods of the attack to networks of the companies. The research has showen that IT specialists are most concerned about two specific types of the attacks: the attacks to refusal in servicing (DoS) and interception (Eavesdropping) — these attacks are specified as the most dangerous and priority approximately at 25% of respondents. And on 15% of respondents chose as key threats of the attack like IP Spoofing and MITM (man-in-the-middle). Other types of threats were priority less than for 12% of respondents.

Today the number of mobile employees and adaptation of policy of usage of own electronic devices for work (BOYD) grows impose new requirements to network safety. At the same time, unfortunately, the number of unsafe network applications very quickly grows. In 2013 the HP company held testing more than 2000 applications as a result of which it was revealed that vulnerabilities in systems of protection have 90% of appendices. This situation poses a serious threat of corporate safety and it isn't surprising that 54% of respondents estimated threats from the malware as the most dangerous.

In the view of the aforesaid, it is possible to draw the following conclusion: modern decisions ensuring network safety among other shall have the following properties:

• to be able to work at the seventh level of the OSI model (at the level of applications);
• to be able to connect the specific user with content of a traffic;
• to have the system of protection against the network attacks (IPS) integrated into the decision
• to support the built-in protection against the attacks like DoS and listening;
• in general to possess high degree of reliability.

Several words about practice of ensuring Information security in our country; let's describe the current legal framework determining aspects of IB in the Russian Federation is short. In the Russian Federation all questions connected with IB are regulated by the following fundamental laws:

• The Federal Law 149 "About information, information technologies and information security";
• The Federal Law 152 "About personal data protection";
• The Federal Law 139 (amendments to the Federal Law 149, the communications act and the Federal Law 436 about protection against information of children);
• The Federal Law 436 (about protection against information of children);
• The Federal Law 187 (about protection of intellectual property and the Internet);
• The Federal Law 398 (about blocking of the extremist websites);
• The Federal Law 97 (about the bloggers who equated them to media);
• The Federal Law 242 (about placement of personal data in the territory of the Russian Federation).

At the same time the laws regulating activities in the areas connected with IB assume serious responsibility for violation of these or those provisions, for example:

• under article 137 Criminal Code of the Russian Federation (illegal collecting or distribution of data on private life of the person) — imprisonment for a period of up to four years;
• under article 140 Criminal Code of the Russian Federation (illegal refusal in provision of the documents and materials collected in accordance with the established procedure) – a penalty or deprivation of the right to hold certain positions or to be engaged in certain activities for a period of 2 up to 5 years;
• under article 272 Criminal Code of the Russian Federation (illegal access to the computer information protected by the law) — imprisonment for a period of up to 5 years.

For most the Russian entities relevance of questions of network safety is connected first of all with the fact that they anyway process data of physical persons (at least, data of the workers). Therefore, irrespective of a type of activity, any company shall consider requirements of the legislation of the Russian Federation and is obliged to apply various organizational and technical measures of protection of information. Specific measures for protection of this or that information are determined in the corresponding Russian IB standards (state standard specification P ISO/MEK 15408, GOST P ISO 27001, etc.), and also regulating documents of the Federal Service for Technical and Export Control (for example, the order of FSTEC No. 58 of 05.02.10 determining methods and methods of protection of the systems processing personal data).

Observance of requirements of the federal legislation by the entities is controlled today by three state bodies: Federal Security Service (FSS), Roskomnadzor and FSTEC. Control is exercised by conducting scheduled and sudden inspections following the results of which the company can be made responsible.

Thus, ignoring of a problem of ensuring network safety in our country can not only yield heavy losses to business, but also entail criminal liability of specific company executives.

Threats of information security become more difficult, hackers and cybercriminals use new acceptances and realize more and more sophisticated attacks for the purpose of breaking of systems and theft of data.

Fight against the new attacks requires solutions on ensuring network safety and development of network strategy of the safety meeting the requirements of reliability, cost and questions of integration with other IT systems. The developed decisions shall be reliable, provide protection against the attacks at the level of applications and allow to identify a traffic.

From all aforesaid a simple conclusion arises – in the modern world it is impossible to ignore questions of information security; in response to new threats it is necessary to look for new approaches to strategy implementation of information security and to use new methods and means of provision of network safety.

УДК 659.3

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

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕКЛАМЕ И PR

Информационная безопасность – набор стратегий для управления процессами, инструменты и мероприятия, необходимые для предупреждения, выявления, документирования и противодействия угрозам цифровой и не цифровой информации. Информационная безопасность заключается в создании набора бизнес-процессов, которые будут защищать информационные активы независимо от того, как формируется информация, является ли она в пути (в момент передачи), находится в процессе обработки или же в состоянии покоя (при хранении).

Программы информационной безопасности строятся вокруг основных целей триады КЦД: сохранение конфиденциальности, целостности и доступности систем и бизнес данных. Эти цели предназначены для того, чтобы конфиденциальная информация раскрывалась только уполномоченным лицам (конфиденциальность), предотвратить несанкционированное изменение данных, обеспечить их достоверность (целостность) и гарантировать, что данные могут быть доступны авторизованным лицам при необходимости (доступность).

Многие крупные предприятия используют специальную группу по безопасности, которая предназначена для внедрения и поддержания программы информационной безопасности организации. Как правило, этой группой руководит старший сотрудник по информационной безопасности. Группа безопасности в соответствии с инструкциями отвечает за проведение управления рисками, за процесс, посредством которого непрерывно контролируются уязвимости и угрозы информационных активов, и за управление применением соответствующих защитных средств.

Согласно работе «Менеджмент в сфере информационной безопасности» А. А. Анисимова, угрозы конфиденциальной и частной информации происходят во многих различных формах, таких как вредоносные программы и фишинговые атаки, кражи личных данных и вымогателей. Фишинговые атаки – это разновидность интернет мошенничества, в основе которого лежит применение социальной инженерии с целью получения конфиденциальной информации о пользователе, зачастую логина и пароля. Для того чтобы удержать нападавших и смягчить уязвимости в различных точках, осуществляются и координируются несколько элементов управления безопасности в рамках многоуровневой защиты. Это должно свести к минимуму последствия атаки. Чтобы быть готовым к нарушению политики безопасности, группы безопасности должны иметь план реагирования на инциденты на месте. Это должно позволить им сдерживать и ограничивать ущерб, устранить причину и применять обновленные средства управления обороны.

Процессы и политики по безопасности данных обычно включают в себя физические и цифровые меры безопасности для защиты данных от несанкционированного доступа,

использования, репликации или уничтожения. Репликация – это копирование данных с одного источника на другой. А. Воеводин в работе «Стратагемы: стратегии войны, бизнеса, манипуляции, обмана» выделяет такие меры как ловушки, управление ключами шифрования, системы обнаружения сетевых вторжений, политики паролей и соответствие нормативным требованиям.

При ведении любой деятельности имеет место конфиденциальная информация, сведения, составляющие коммерческую тайну, а отсюда и возможность возникновения каналов утечки подобной информации.

Коммерческая тайна – это своего рода конкурентное преимущество компании, ее собственность. Согласно статье 139 Гражданского кодекса Российской Федерации «коммерческую или служебную тайну составляет информация в случае, если она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры по охране ее конфиденциальности».

Ответственными за предоставленную информацию и соблюдение всех требований в сфере информационной безопасности являются составители информации, специальные структурные подразделения и соответственно руководители фирмы.

К основным задачам в сфере защиты информации в рекламной и пиар деятельности отнесем: анализ и экспертиза информации, предназначенной для обнародования, проверка данных на отсутствие в них каких-либо сведений с ограниченным доступом; постоянный или периодический контроль за размещением рекламных и пиар материалов, их обнародованием, содержанием.

При организации деятельности в сферах рекламы и пиара, должностное лицо, ответственное за распространение рекламной информации, обязано организовать работу, цель которой — предотвращение распространения конфиденциальной информации.

Некоторые нарушения при ведении рекламной деятельности могут привести к привлечению ответственности по закону, поэтому необходимо иметь достаточный уровень знаний в сфере рекламного законодательства, которое тесно взаимодействует с законами об авторских правах, о защите прав потребителей, о правах на средства индивидуализации.

Существуют основные заблуждения, которые могут привлечь внимание антимонопольных служб. Главная опасность этих заблуждений заключается в том, что формальный подход к рекламе, пиару не всегда является правильным, то есть законным.

Например, существует прием замены какой-либо буквы апострофом. Также используется многоточие вместо известных всем трех букв, что также противоречит законодательству. В рекламе и PR заключительное значение имеет восприятие информации с точки зрения населения.

Делать так, как другие и надеяться, что все пройдет безнаказанно – это суть следующего заблуждения. Если отдельная компания не была привлечена к ответственности, нет стопроцентной гарантии, что ее действия законны. Или же, взяв за основу продукт другой компании, ввести в него даже незначительные корректировки, можно кардинально изменить его восприятие в лучшую или худшую для себя сторону.

Следующее заблуждение имеет такой смысл - большинство действуют не по правилам, в общей массе собственные нарушения будут незаметны. Действительно, нарушения в сфере пиара и рекламы набирают рост, и вполне возможно, что контролирующие органы упустят из виду вашу деятельность, однако стоит помнить о конкурентах. Поэтому лучше оплатить работу юриста за анализ публичной информации, чем выплачивать штраф за нарушения.

Исходя из вышеописанного, следует принимать меры с целью повышения уровня обеспечения информационной безопасностью, что напрямую зависит от проработанности законодательной базы, развития инновационно-коммуникационных технологий. От того, насколько изучены проблемы информационной безопасности, проработаны механизмы защиты информационного пространства, зависит безопасность и будущее место организации в маркетинговой среде.

УДК 005:338.001.36

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

О КРИЗИСНЫХ ЯВЛЕНИЯХ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ

В трактовке термина «социально-экономическая система» отсутствует единство взглядов, что обусловлено разнообразием и сложностью таких систем. Рассмотрим авторский подход к определению этого термина с позиций системного анализа.

Социально-экономическая система (СЭС) – это конечное множество элементов (субъектов и объектов системы) и отношений между ними, характеризующихся конкретными функциями, связанными с процессами производства, обмена, распределения и потребления результатов труда, выделенное из среды и определяемое конкретной целью (или несколькими целями) в рамках фиксированного интервала времени, называемого жизненным циклом системы.

Краткое описание содержания термина «социально-экономическая система» и механизмов, проходящих в СЭС.

У каждой СЭС есть следующие системные характеристики:

Атрибутами СЭС являются: элементы СЭС (субъекты и объекты); отношения между элементами СЭС (причем, между двумя элементами СЭС может быть несколько отношений); системная цель (системные цели), которые будут подробнее описаны ниже; системные функции, определяемые системными целями; жизненный цикл СЭС, продолжительность во времени которого определяется всеми остальными атрибутами СЭС, а также эволюционирующей под влиянием внешних и внутренних воздействий структурой СЭС.

Любая СЭС перманентно взаимодействует с внешней средой, которую будем называть универсумом. Атрибуты СЭС и каждое ее взаимодействие с универсумом определяют реакцию СЭС на конкретное воздействие на систему со стороны универсума. Такую реакцию назовем механизмом адаптации СЭС на конкретное воздействие на систему со стороны универсума. Такие механизмы адаптации СЭС способствуют повышению ее жизнестойкости (процессы системной самоорганизации) и определяют вектор эволюции системы 1-го вида.

Кроме того, внутри СЭС возможны воздействия на ее структуру со стороны элементов (субъектов СЭС). Поэтому существует адаптация СЭС к процессам взаимодействия между элементами СЭС (субъектами СЭС), участвующая в формировании новых отношений между элементами СЭС, которые определяются функциями и целями мыслящих элементов системы (эволюция СЭС 2-го вида). Эту адаптацию также отнесем к процессам системной самоорганизации.

Процессы самоорганизации в СЭС являются результатом человеческой деятельности (воздействий на СЭС, как со стороны универсума, функционирование которого в большинстве своем детерминировано людьми, так и со стороны элементов – субъектов СЭС).

Оба вида эволюции СЭС в синергетическом взаимодействии определяют итоговый вектор развития СЭС в рамках существующей цели (существующих целей) системы и ее элементов (субъектов СЭС), который ограничивается возможностями существующей структуры СЭС.

Отношения между элементами СЭС и СЭС и универсумом носят не только экономический характер (т.е. отношения связанные с процессами производства, обмена, распределения и потребления результатов труда). В процессе эволюции СЭС возникают и развиваются отношения между элементами СЭС и СЭС и универсумом, которые носят социальный характер. Хотя на междисциплинарном уровне большое количество исследователей указывают на связь между социальными и экономическими проблемами человечества, пока будем разделять эти отношения.

Функции СЭС определяются направлением и способами ее активности по отношению к универсуму исходя из системной цели (системных целей) СЭС.

Системные цели СЭС бывают двух видов: цель (цели) во взаимоотношениях с универсумом и цель (цели) во взаимоотношениях между элементами (субъектами СЭС) по отношению их к самой системе. В современных условиях динамично изменяющейся внешней (по отношению к СЭС) среды (универсума) системные цели также динамично меняются, что приводит к изменениям в самой системе. Эти системные цели могут изменяться не только по их векторной направленности, но и по количеству самих целей. Это обусловлено не только изменениями во внешней среде, но и изменениями целей у множества экономических агентов,

являющихся элементами системы. При этом цели экономических агентов (элементов СЭС) и самой системы не всегда совпадают. Экономические агенты (элементы СЭС) имеют определенную независимость в пределах системы, что дает им возможность самостоятельно принимать решения для достижения своих индивидуальных целей. Это приводит к возникновению конфликтов между агентами (элементами СЭС), а также к несоответствию интересов агентов (элементов СЭС) с общими целями системы.

Структура СЭС – это сложная конструкция, которая, как правило, состоит из элементов СЭС и отношений между ними и соответствует системной цели (системным целям) СЭС. Но в самом общем случае требуется уточнение содержание этой системной категории с привязкой этого содержания к конкретной СЭС. Структура СЭС во многом определяет ограничения в ресурсах СЭС и, следовательно, возможности процессов самоорганизации в СЭС, как по векторной направленности, так и по их содержанию.

Краткое описание кризисных явлений, проходящих в СЭС

В процессе эволюции СЭС возникают конфликтные ситуации. Опишем самые распространенные из них: конфликт между системными целями СЭС и воздействиями на нее со стороны универсума; конфликт между возможностями структуры СЭС к дальнейшей эволюции и воздействиями на СЭС со стороны универсума, не соответствующими существующей структуре СЭС; конфликт между целями СЭС и целями ее элементов (субъектов СЭС). Этими видами список конфликтных ситуаций в СЭС не исчерпывается.

Случаи, когда конфликтная ситуация приводит к существенной деформации структуры СЭС (именно структура СЭС определяет возможности СЭС при ее адаптации к воздействиям), назовем кризисным явлением, проходящим в СЭС. При этом, как правило, существенно изменяются атрибуты СЭС (как по количеству, так и по содержанию: например, системные цели СЭС). В таком случае СЭС прекращает свое существование в прежнем виде – жизненный цикл СЭС заканчивается.

Перечислим основные виды прекращения СЭС:

1. СЭС реорганизуется в другую СЭС. Например, при реорганизации предприятия, как правило, изменяется не только его организационно-правовая форма, но и количество элементов СЭС, отношений между ними, системные цели и т.д. Но это уже другая СЭС, исходя из определения, сформулированного в начале работы.
2. СЭС физически перестает существовать (например, развал СССР как цельной социально-экономической системы или, если на микроуровне – банкротство конкретного субъекта хозяйствования).

Дальнейшие исследования позволят наполнить конкретным содержанием каждое из положений работы, которые здесь представлены конспективно.

УДК 338

Кутузов Валерий Васильевич
к.ф.-м.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

УСЛОВИЯ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЯ СТРОИТЕЛЬНОЙ ОТРАСЛИ

Введение. Предложен абстрактный подход к надежному функционированию предприятия строительной отрасли. Построена функциональная модель, связывающая рентабельность, удельные переменные затраты, удельную цену и параметр, согласовывающий постоянные затраты и объем производства.

Цель и задачи исследования. Проанализировать рентабельность как результат действия основных факторов производства в предположениях, позволяющих четко разграничить постоянные и переменные затраты.

Результаты исследования. Рассмотрим производственную деятельность некоторой фирмы, интересы которой относятся к строительной сфере. Как известно, в общем случае разделение затрат на постоянные и переменные представляет достаточно сложную задачу. Особенность строительного производства позволяет сделать некоторые допущения: пусть полные затраты за выделенный период T составляют r рублей, переменные затраты Z пропорциональны объему строительства V ,

$$Z = z_1 * V \quad (1)$$

где z_1 - переменные затраты на производство единицы (1 кв.м.площади) строительной продукции (удельные переменные затраты). Отметим, что величины r и V являются согласованными: объем выполненных заказов на строительство V должен быть осуществлен за тот период Т, за который рассчитаны постоянные затраты П. Надежность работы предприятия предполагает его рентабельность. Предположим, что выручка W предприятия формируется как произведение договорной цены единицы строительной продукции (руб./кв. м.) на объем строительства,

$$W = p_1 * V \quad (2)$$

(V - весь объем строительства за рассматриваемый период Т). На основе рассмотренных показателей возможно получить рентабельность R предприятия:

$$R = \frac{p_1}{z_1 + f} \quad (3)$$

Здесь для уменьшения громоздкости формулы принято обозначение

$$f = \frac{П}{v}. \quad (4)$$

Размерность параметра f руб./кв. м., он соотносит общий объем заказов к постоянным затратам за один и тот же период T. В правой части формулы (3) показатели p_1, z_1 и параметр f имеют одинаковую размерность - руб./кв. м., правая часть размерности не имеет, рентабельность выражена числом. Например, если в правой части получаем 0,1, значит рентабельность, как она трактуется в экономике, будет 10%.

Выводы. Об экономическом смысле формулы (3). Рентабельность увеличивается при увеличении договорной цены на единицу строительной продукции (p_1). Однако повышение этого показателя ухудшает конкурентные возможности предприятия. Увеличивается рентабельность и при уменьшении удельных переменных затрат (z_1) и уменьшении параметра f, балансирующего соотношение заказов и постоянных затрат. Можно отметить, что оба эти фактора по степени влияния на рентабельность равнозначны.

УДК 658:004.056

Потанина Марина Викторовна
к.т.н., доцент
Байздренко Екатерина Александровна
к.т.н., доцент
Писарюк Светлана Николаевна
к.э.н., доцент
Институт финансов, экономики и управления
ФГАОУ ВО «Севастопольський государственный университет»
Республика Крым, Россия

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В КРУПНЫХ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЯХ

Объем электронного документооборота в больших коммерческих организациях в настоящее время достигает огромной величины. Это создает определенные трудности по его сортировке и контролю. Особенно, если предприятие имеет территориально разделенные подразделения. Сотни работников предприятия и его подразделений каждый день обмениваются электронными письмами, к которым прикреплены различные вложенные документы. На предприятии происходит активный анализ различных документов и обзоров из Интернета, отправляется информация из баз данных предприятия, информация коммерческого направления, всевозможные формы отчетности и др. Зачастую эта информация является конфиденциальной и имеет определенную коммерческую ценность для предприятия. К подобной информации можно отнести маркетинговые, финансовые данные предприятия. Подобная информация часто носит также авторский характер.

Возникает проблема управления информационной безопасностью коммерческой информации предприятия, проблема защиты электронного документооборота.

Существуют различные способы обеспечения информационной безопасности электронного документооборота крупных предприятий и методы управления ею. Первым рубежом защиты является локальная политика безопасности предприятия. Она позволяет с помощью определенных технологий, например технологии «электронной подписи» отслеживать внутреннюю корпоративную почту. Этим обычно занимается служба безопасности предприятия. К сожалению, при огромном количестве сотрудников, приходится такие проверки производить выборочно.

В настоящее время пользователи очень активно используют «Облачные файлообменники» или личные, а не корпоративные, почтовые ящики для работы. С их помощью они пересылают служебную информацию, читают, копируют и печатают документы. Отследить все это неконтролируемое распространение ценной финансовой, коммерческой и маркетинговой информации компании без специального программного обеспечения практически невозможно. Таким образом, подобная конфиденциальная информация может выходить за пределы организации.

Очевидно, что если предприятие теряет финансовую или маркетинговую конфиденциальную информацию в результате утечки или взлома, то это может, как нанести существенный вред репутации предприятия, так и привести к крупным финансовым потерям. Потеря или кража ценной коммерческой информации компании может повлечь за собой проблемы в конкурсах и тендерах, привести к опережению её конкурентами.

Предлагается использовать профессиональные комплексы решений для защиты электронной переписки и конфиденциального документооборота различного рода в крупных компаниях и корпорациях. Профессиональное программное обеспечение позволит иметь доступ к почте только его получателю, защищать цифровую информацию и электронные документы от копирования, нелегального доступа и использования, то есть работать непосредственно с контентом.

Также важно применять программы для контроля деятельности сотрудников предприятия. Подобные программы отслеживают доступ сотрудника к файлам и папкам, произошедшие изменения файлов, отправку документов на печать, использование USB-накопителей, время работы с конкретными приложениями, ввод данных в программах мгновенных сообщений и т.п. Все это может быть программно зафиксировано, что позволяет создавать отчеты для системного администратора, сотрудника службы безопасности или аналитика компании, обеспечивающих информационную безопасность.

В случае подозрения на инсайдерский инцидент или утечку информации, служба безопасности компании будет располагать информацией о полном спектре действий, осуществляемых персоналом. Подробные отчёты о работе сотрудника с файловой системой, реестром, периферийными устройствами, эффективны для ретроспективного анализа и расследования, а также предупреждения инсайдерских инцидентов.

На основании отчётов о времени работы сотрудников – в общем, и с каждым приложением в отдельности, о данных, вводимых в тех или иных приложениях, возможно осуществление точного контроля действий персонала предприятия: контроль над использованием трудовых ресурсов и стимулирование трудовой дисциплины сотрудников.

Использование политик доступа к конфиденциальной информации и информирование персонала о том, что все его действия на компьютере регистрируются, является одним из наиболее эффективных средств защиты информации в настоящее время.

Подобные профессиональные программные продукты предлагают ряд компаний сферы информационной безопасности, в том числе и российских. Такие инновационные решения позволят грамотно организовать систему защиты электронного документооборота и контроля распространения защищенного материала в крупных коммерческих организациях, эффективно управлять информационной безопасностью.

УДК 519.237

Руденко Людмила Ивановна,
к.ф.-м.н., доцент
Пушкарева Елена Викторовна,
старший преподаватель
ФГАОУ ВО «КФУ имени В. И. Вернадского
Республика Крым, Россия

АНАЛИЗ СТРУКТУРЫ КОЛЛЕКТИВА МЕТОДАМИ МНОГОМЕРНОГО ШКАЛИРОВАНИЯ

Анализ структуры коллектива является отправной точкой в оценке его работоспособности и наличия в нем положительного психологического климата, существенно влияющего на характер деловых взаимоотношений. Структурные особенности дают повод для оценки устойчивости команды к воздействию неблагоприятных факторов, в том числе, и сточки зрения информационной безопасности при определенных видах деятельности. Выявленная структура коллектива позволяет также формировать эффективные команды для решения поставленных задач или создавать в рамках коллектива группы целевого назначения. Так, в учебном коллективе такие задачи могут возникнуть при делении на подгруппы для прохождения практики, для участия в проекте или соревнованиях и т. д.

Один из подходов к решению таких задач основан на применении методов анализа данных, а именно методов многомерного шкалирования.

Многомерное шкалирование (*Multidimensional Scaling*) представляет собой группу методов и алгоритмов анализа данных, основным результатом которых является воссоздание некоторого многомерного пространства. Оси пространства называются шкалами, откуда и следует название методов. Воссозданное пространство является моделью пространства восприятия респондентов, в котором они выражают свои предпочтения к исследуемым объектам. Главная особенность состоит в том, что свойства объектов не выражаются количественными оценками, а зачастую и не поддаются описаниям.

Так, в области внутриколлективного взаимодействия возникают задачи исследования мнений, настроений, конфликтов и других ситуаций с невыраженными количественными оценками. И здесь применение методов многомерного шкалирования представляется вполне уместным и результативным.

Итак, задача многомерного шкалирования состоит в воссоздании латентного пространства, в котором размещаются исследуемые объекты. И в отличие от традиционных методов статистики, опирающихся на данные типа «объект – признак», за основу берутся данные вида «объект – объект»: их парные сравнения, оценки сходства или различия. Воссозданное пространство небольшой размерности позволяет наглядно представить расположение объектов, что способствует формулировке выводов и принятию решений.

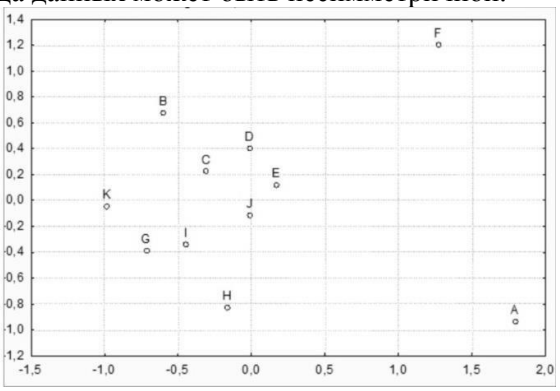
Основные идеи и математическое обоснование методов многомерного шкалирования были предложены в середине XX века в работах М. У. Ричардсона, Л. Л. Терстоуна, У. С. Торгерсона (метрические алгоритмы), Р. Н. Шеппарда, Дж. Б. Краскала (неметрическое шкалирование).

Суть методов кратко можно описать так. Для n объектов некоторым способом получена матрица сходства (различия) Δ. В пространстве восприятия размерности k требуется получить координаты объектов. Матрица координат X размерности $n \times k$ связана с матрицей данных соотношением $\Delta = XX^T$ (теорема Терстоуна). Отсюда, используя методы факторного анализа, можно восстановить требуемые координаты. Расстояния в восстановленном пространстве должны соответствовать оценкам близости исходных объектов. Мера соответствия устанавливается с использованием так называемых «стресс-формул» (Краскал, Гутман), а визуально оценивается с помощью диаграммы Шеппарда. Главный результат – получение геометрической конфигурации объектов в пространстве размерности 2 или 3, по которой можно интерпретировать структуру множества объектов, наличие в нем классов объектов, выбросов и других особенностей.

Пример. Рассмотрим анализ структуры коллектива академической группы учебного заведения путем воссоздания двумерного пространства и расположения в нем образов объектов (учащихся). Эмпирическими данными являются данные опроса в реальной группе учащихся, фамилии которых заменены символами *A, B, C* и т. д. В данном примере это оценки, выставленные каждым членом группы в шкале от 0 до 9 (возможны иные градации) другим

учащимся из данной группы по степени желания совместно работать в одной команде. Все оценки внесены в таблицу (*а*). Заметим, что матрица данных может быть несимметричной.

	A	B	C	D	I	F	G	H	I	J	K
A	0	3	6	6	6	3	2	5	5	6	0
B	0	0	7	9	5	0	8	6	8	5	9
C	1	9	0	9	7	1	9	9	9	8	8
D	2	9	9	0	7	1	8	7	9	7	7
E	5	7	9	9	0	5	7	9	9	9	9
F	4	3	6	6	6	0	8	9	4	0	8
G	0	7	9	8	8	0	0	7	9	5	9
H	2	5	9	9	6	5	8	0	9	7	9
I	1	6	9	9	6	5	9	9	0	7	8
J	6	9	9	9	9	0	9	6	9	0	9
K	0	6	8	8	6	2	9	8	8	8	0



(*а*) Эмпирические данные. (*б*) Итоговая конфигурация.

Итоговая конфигурация в воссозданном двумерном пространстве, полученная с использованием специализированного статистического приложения, приведена на иллюстрации (*б*). Она характеризует вполне интерпретируемую структуру группы: в целом достаточно сплоченное ядро, за исключением двух объектов с кодами *A* и *F*, которым, как видно в столбцах таблицы (*а*), были выставлены более низкие баллы. Заметим, что в других группах по результатам опроса было отмечено разделение на две подгруппы либо отсутствие явной структуризации, что также допускает свою интерпретацию.

УДК 004.056

Рыбников Андрей Михайлович
к.э.н., доцент
Рыбников Михаил Сергеевич
к.ф.-м.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Проблемы информационной безопасности в современных условиях являются чрезвычайно актуальными и требуют углубленного изучения. Термин "безопасность" понимается как состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз. Но его содержание в научном понимании еще в полной мере не определено. Сегодня идет дискуссия вокруг этого вопроса, в частности вокруг оценки критериев безопасности, характеристик вероятных опасностей и их структуры или принципов построения системы обеспечения безопасности, как государства в целом, так и каждого его отдельного предприятия.

Как известно, деятельность любого хозяйствующего субъекта связана с большим количеством разнообразных рисков, особенно в условиях рыночной экономики. Основными задачами руководства предприятия становится поиск оптимальных управленческих решений для выхода из кризисных ситуаций или смягчения их негативного воздействия на отдельные аспекты деятельности и предприятия в целом, т. е. достижение состояния экономической безопасности хозяйствующего субъекта.

Такие задачи невозможно решить без тщательной подготовки и проработки всех возможных вариантов развития событий. Для принятия эффективного решения руководству необходимо учитывать множество факторов, то есть иметь основательную информационную базу.

В современных условиях все большее значение приобретает информационное обеспечение, которое представляет собой сбор, обработку и предоставление руководству информации, необходимой для принятия обоснованных управленческих решений. Именно от информации, ее своевременности, достоверности, полноты, правильной интерпретации часто

зависит эффективность деятельности предприятия, его безопасность, конкурентоспособность, а иногда и факт существования на рынке.

Следовательно, на любом современном предприятии жизненно необходимо существование системы информационного обеспечения, которая будет включать экономическую разведку, информационную безопасность и аналитически-консультативное обеспечение.

Экономическая разведка должна обеспечивать сбор информации, группировку, обработку и предварительный анализ собранных данных. Достоверность собранной информации, а также степень доверия к ней оказывает значительное влияние на дальнейший анализ и выработку рекомендаций по действиям в конкретных ситуациях. Кроме того доступ к разведывательным и аналитическим данным должен быть ограниченным, что уменьшит вероятность утечки информации и использования ее в ущерб данному предприятию. Решение этих вопросов касается сферы информационной безопасности.

Ведущую роль в информационном обеспечении играет, на наш взгляд, аналитически-консультативное обеспечение, которое осуществляет продвижение материалов разведки до конечного потребителя или заказчика, то есть руководства предприятия. Основными задачами аналитико-консультативного обеспечения должны быть:

1. Глубокий анализ полученных данных, сопоставление их с имеющейся информацией, фактами, событиями, выявление взаимосвязей.
2. Прогнозирование развития событий с максимальным количеством возможных вариантов, выявление последствий влияния таких событий на предприятие в целом и его окружающую среду.
3. Отработка предыдущих управленческих решений по каждому вероятному варианту развития событий.
4. Проведение консультаций руководства предприятия по любому вопросу.

Основной задачей создания на предприятии системы информационного обеспечения является достижение состояния экономической безопасности, что в свою очередь достигается путем решения следующих задач:

- владение наиболее полной информацией об окружающей среде и внутреннюю среду предприятия;
- моделирование и прогнозирование различных вариантов развития событий;
- отработка предыдущих управленческих решений по каждому из вариантов развития событий;
- обеспечение сохранности информации и предотвращения ее утечки;
- принятие обоснованных управленческих решений;
- максимальное использование благоприятных факторов для деятельности предприятия и устранение или ослабление опасностей и угроз.

Правовое обеспечение информационной безопасности должно основываться прежде всего на соблюдении принципов законности и баланса интересов в информационной сфере. При этом соблюдение принципа законности требует при разрешении конфликтов, возникающих в информационной сфере, неукоснительно руководствоваться законодательными и иными нормативно-правовыми актами, регулирующими отношения в этой сфере. Соблюдение принципа баланса интересов в информационной сфере предполагает использование различных форм общественного контроля в деятельности соответствующих подразделений предприятия. Реализация гарантий прав и свобод, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационного обеспечения безопасности.

УДК 004.056

Сурнина Екатерина Станиславовна
д.э.н., профессор
Аблаева Тамила Дамировна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И.Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

На сегодняшний день коммерческие банки представляют собой важнейший финансовый институт кредитно-финансовой системы Российской Федерации, а также современного общества, в связи с этим они должны соблюдать правила информационной безопасности с целью противостояния дестабилизирующим факторам. Многократное возрастание стоимости и значимости банковской информации привело к возрастанию преступного интереса к ней. Целью обеспечения информационной безопасности является защита информации банка и бизнес процессов для обеспечения его долгосрочной деятельности и безопасности.

Каждый банк должен обеспечивать безопасность данных, принятых на хранение, в связи с чем, он обязан регулярно следить за сменой, проверкой паролей и осуществлять контроль вероятности утечки информации. Банковские базы данных включают конфиденциальную информацию о клиентах, проводимых операциях и состоянии их счетов, поэтому необходимо обеспечивать сохранность таких данных и информационную безопасность.

Основой угрозой информационной безопасности банка является человеческий фактор, утечка информации во многих случаях вызвана халатностью, мошенническими действиями сотрудников банков, непосредственно имеющих доступ к данным. Помимо внутреннего фактора, возможны технические угрозы информационной безопасности банка – взломы информационных систем лицами, которые не имеют прямого доступа или криминальными организациями. Существует разнообразие форм взлома информационных систем, одной из современных форм является применение электромагнитных и электрических излучений для получения конфиденциальной информации.

Компьютерные системы являются необходимым средством осуществления работы в банке, но вместе с тем представляют серьезную угрозу для осуществления технических атак. Опасность для программного обеспечения представляют вредоносные вирусы, программные закладки, разрушающие введенные коды.

Выделяют несколько типовых видов атак в банковской сфере:

- атаки на системы «front-end». Данный вид атак направлен на манипулирование с транзакциями, в том числе, и с финансовыми, например, атаки на терминалы, банкоматы. Данный вид атак не получил широкого распространения, так как обеспечение защиты транзакционных систем основано на применении криптографических алгоритмов, как для электронной подписи так и для шифрования. Единственное, чему необходимо уделить внимание – надежной системе распределения ключей, физической безопасности терминалов;
- атаки на системы «back-office». Этот вид атак наиболее популярный и осуществляется и внешними и внутренними злоумышленниками. Такие атаки представляют манипуляции с базами данных, осуществляемые как с применением приложений, так и напрямую. Для противодействия используется широкий круг мер: проведение мониторинга и аудита, физическая безопасность, управление доступом, разделение среды разработчиков и организационной среды, организационные меры.

К коммерческим банкам со стороны регулирующих органов предъявляются разнообразные требования и рекомендации по обеспечению информационной безопасности, в частности постановления и инструкции ЦБ РФ, отечественные и международные стандарты. Среди основных элементов информационной безопасности банка выделяют:

- осуществление авторизации и аутентификации;
- обеспечение защиты от несанкционированного доступа к системам и обеспечение внутренней защиты сотрудников банков от несанкционированного доступа;
- обеспечение защиты каналов передачи информации, сохранение целостности и актуальности данных во время обмена информации с клиентами;
- обеспечение юридической значимости электронных документов;

— управление инцидентами информационной безопасности;
— проведение внутреннего и внешнего аудита системы информационной безопасности.

Обеспечение информационной безопасности является непрерывным процессам, а меры должны иметь комплексный и превентивный характер. Эффективная защита невозможна без осуществления организационных мер, в ходе которых определяются цели, приоритеты, задачи, риски в области информационной безопасности и, учитывая эти факторы, формулируются требования, разрабатывается политика и система управления информационной безопасностью. Технические средства защиты выбираются на основании предварительного анализа возможных рисков.

Таким образом, формирование системы информационной безопасности банка начинается с комплексной диагностики основных бизнес-процессов и информационной системы, а также инструментов обеспечения информационной безопасности. Результатом осуществления диагностического обследования, кроме разработки предложений и рекомендаций, может быть спроектированная система информационной безопасности.

Защита данных банковской системы является комплексом мероприятий, начиная от аудита до разработки концепций по защите различных банковских служб. Меры защиты информации позволяют снизить вероятности реализации рисков и угроз определенного класса информации.

Одним из способов защиты информации является контроль за прохождением и регистрацией секретной информации, а также установление безопасных альтернатив по обмену файлами внутри банка. Для обеспечения защиты также используются концепции идентификации, которые характеризуют наличие прав доступа к информации. Для этих целей применяется система паролей для входа в систему, а также система электронных ключей.

Таким образом, ввиду экономической важности банковских систем, обеспечение информационной безопасности является необходимым условием. Так как информация, содержащаяся в банковской базе данных, имеет материальную стоимость, то и требования по хранению и обработке будут всегда повышенными. Особенности организации системы информационной безопасности являются индивидуальными для каждого банка, но комплексное обеспечение информационной безопасности отдельного банка является важным условием эффективной работы всей банковской системы Российской Федерации.

Титаренко Дмитрий Викторович
к.э.н., доцент
Алексеева Н. А.
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ МЕНЕДЖМЕНТА КАЧЕСТВА ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ

Человечество стремиться обезопасить себя во всех сферах своей жизнедеятельности. Начиная от здоровья и заканчивая безопасным серфингом на просторах Интернета, на каждое из этих действий человек старается снизить риск опасности. Для этого ученые разрабатывают новые препараты для лечения болезней, придумывают менее опасные технологии изготовления продукции, с младенчества учат детей правилам безопасности. С развитием технологий специалисты вынуждены осваивать все новые отрасли, которые теперь тоже нуждаются в защите. Технический прогресс упростил многим жизнь, с легкостью можно найти необходимую тебе информацию, уменьшилось количество бумажных хранителей, появились облачные технологии хранения, можно бесконечно перечислять преимущества, однако есть и недостатки. Одним из них является и появление взломщиков ПО и злоумышленников крадущих персональные данные и важные документы. Встал острый вопрос защиты и безопасности информации, так развилось понятие информационная безопасность. В Российской Федерации основной документ регламентирующий безопасность в информационной сфере называется «Доктрина информационной безопасности Российской Федерации» и в ней дано следующие определение:

«Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и

устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Одним из основных свойств информационной безопасности выступает конфиденциальность. То есть доступ к данным может получить только авторизированный и опознанный пользователь, остальные пользователи никак не могут получить доступ к файлам. Соответственно злоумышленникам перекрыт путь.

Органы местного самоуправления как одна из форм публичной власти нуждается в информационной защищённости данных. Эффективность деятельности таких организаций непосредственно зависит от уровня защищенности данных. Такой громоздкий процесс как информационная безопасность должен быть описан и регламентирован документально. Обеспечение качественной защиты данных и гармоничного внедрения информационной безопасности в основные процессы органов местного самоуправления следует внести в систему менеджмента качества.

Рассмотрим этапы разработки СМК (системы менеджмента качества) фокусируя внимание на информационной защите:

1) Проведение анализа действующей системы менеджмента качества на предприятии. Так же проводится аудит в ИТ отделе и определяется уровень защищенности организации.
2) Улучшить уже существующую СМК или определить основы для новой СМК. Улучшения должны затрагивать и безопасность информации.
3) Внедрение улучшенной или новой СМК, с внесёнными в неё изменениями.
4) Провести сертификацию СМК.
5) Поддерживать работоспособность системы и постоянно проводить мониторинг уровня информационной безопасности.

Информационная безопасность является неотъемлемым условием для эффективной и целостной работы органов местного самоуправления. Так же следует регламентировать методы информационной защиты в системе менеджмента качества, действующей в муниципальном образовании. Ведь от качества предоставляемой защиты, напрямую зависит работоспособность всей организации.

Титаренко Дмитрий Викторович
к.э.н., доцент
Матюх Анастасия Юрьевна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УПРАВЛЕНИИ ЗАПАСАМИ

XXI век – век информационных технологий во всех сферах жизни человечества. Современные предприятия для организации эффективной работы и повышения производительности вынуждены совершенствовать свои механизмы работы с объектами, содержащими информацию. На сегодняшний день информация - это нечто больше, чем просто данные. Это оружие, активно используемое в политике, экономике, науке и технике. Это стратегический ресурс, производительная сила, что вызывают стремление государства, предприятий и отдельных граждан завладеть информацией и получить преимущество для достижения поставленных целей. Для каждого предприятия одной из самых важных задач является обеспечение информационной безопасности. Ведь ее нарушение ведет к различным внешним и внутренним угрозам для деятельности предприятия.

Рассмотрим проблему информационной безопасности с точки зрения управления запасами на предприятии. Системы управления запасами могут позволить снизить уровень затрат на закупку запасов, наладить работу с поставщиками, контролировать транспортные расходы и уровень обслуживания покупателей. Все это достижимо, если информация, которая накапливается в этой системе, будет рационально использована и надежно защищена. Защита информации должна обеспечивать три базовые задачи:

1. Целостность данных. Информация должна быть защищена от неправомерного доступа, сбоев, ведущих к ее потере, блокирования, распространения и других неправомерных действий. В управлении запасами очень важна правильная и точная работа системы, без

сбоев и ошибок, так как поставка запасов точно в срок и своевременное исполнение заказов – главные конкурентные преимущества.

2. Соблюдение конфиденциальности информации. Незаконное разглашение, утечка и повреждение информации. При создании системы управления запасами используется информационный подход к решению проблемы. Информация принимается, обрабатывается, фильтруется, передается и в результате формируется основа для будущего управленческого решения. Разработка системы управления запасами – трудоемкий процесс анализа, моделирования и реализации. А действующая система – это прежде всего ценная информация, обеспечивающая успешную деятельность, которая непременно будет вызывать интерес у предприятий-конкурентов, а также желание получить и воспользоваться ею. К примеру, утечка информации о поставщиках, может позволить конкурентам делать закупки дешевле у других поставщиков, при этом снижать стоимость аналогичного товара.
3. Доступность информации – субъекты, имеющие право доступа, могут влиять на состояние информации. Информация в системе управления запасами должна быть доступна конкретным лицам, имеющим непосредственное отношение к планированию, закупкам, складированию и ведению учета.

Нарушение одного из этих правил может негативно сказаться на работе предприятия. Поэтому особо важным этапом в разработке системы управления запасами, которым не стоит пренебрегать, является обеспечение информационной безопасности через реализацию механизмов защиты. Предлагается принимать некоторые распространенные меры защиты систем информационной безопасности: обеспечение надежного хранения данных на различных носителях, ограничение доступа к некоторым данным, защита информации при ее передаче по каналам связи, создание резервных копий, установка антивирусной защиты и др.

Любая система нуждается в максимально эффективной защите информации, так как в современном обществе именно информация играет очень важную роль в успешной и продуктивной деятельности компании.

Титаренко Дмитрий Викторович
к.э.н., доцент
Никитина Виктория Николаевна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В работе рассмотрены понятия системы менеджмента информационной безопасности, основные угрозы для безопасности информации, мероприятия по обеспечению информационной безопасности на предприятии.

Ключевые слова: система менеджмента информационной безопасности, информация, информационная безопасность.

Информационная безопасность предприятия предполагает поддержание целостности информации от момента её создания до момента уничтожения или до потери значимости информации для предприятия, предотвращение распространения информации или её изменения, которое может нанести вред деятельности предприятия. Наиболее действенным инструментом защиты данных является система менеджмента информационной безопасности.

Цель: рассмотрение понятия «система менеджмента информационной безопасности», определение основных угроз информационной безопасности предприятия и основ обеспечения информационной безопасности на предприятии.

Понятие «информационная безопасность» определяет такой исход событий, при котором целостность данных не нарушена и любой несанкционированный доступ к данным, в том числе с помощью современных технологий и специальных устройств, не возможен. Конечно же на практике идеальную защиту информации обеспечить не возможно, т.к. способы добычи необходимой информации постоянно совершенствуются. В связи с этим целью информационной безопасности является минимизация ущерба.

Выделяют три основные угрозы информационной:

1. Политика государства в сфере регулирования деятельности предприятия/организации;
2. Действия разных субъектов рынка (конкуренция, шпионаж, попытка захвата большего объёма потребителей посредством производства совершенно нового товара, и т.д.);
3. Кризис (как внутри страны, так и мировой).

Для эффективной защиты важных данных, а также минимизации возможного ущерба предприятию, необходимо разработать систему информационной безопасности, которая бы обеспечивала мониторинг всех стадий создания товара, отслеживала и участвовала в обеспечении деятельности всех подразделений предприятия, осуществляла сбор данных о всех возможных угрозах безопасности данных, как внутренних, так и внешних), и совершенствовала методы защиты, анализируя имеющиеся и получаемые данные.

Процесс создания такой системы зачастую включает следующие стадии:

1. Анализ реальной обстановки на рынках разных уровней, выявление существующих и потенциальных угроз информационной безопасности;
2. Оценивание выявленных угроз и определение степени возможного ущерба;
3. Разработка мер, обеспечивающих защиту данных от выявленных угроз;
4. Реализация разработанных мер, предотвращение ущерба деятельности предприятия или его минимизация, сбор данных от реализации разработанных мер и, при необходимости, усовершенствование созданной системы.

В зависимости от формы собственности предприятия, характера и сферы деятельности, масштабности и других факторов, процесс обеспечения информационной безопасности может быть усложнён и включать больше этапов.

Халилова Фатиме Ситмеметовна
к.п.н., старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ CRM-СИСТЕМЫ ДЛЯ ОБРАЗОВАТЕЛЬНОГО РЕСУРСНОГО ЦЕНТРА ВУЗА

CRM-система (Customer Relationship Management - управление отношениями с клиентами) - корпоративная информационная система, незаменимый современный инструмент для ведения бизнеса. Она дает возможность не просто автоматизировать взаимодействие с клиентами и процесс продаж, а выстроить их работу таким образом, чтобы получать максимальный результат. CRM-системы в России появились сравнительно недавно, попыткой автоматизации процесса учета и контроля в образовательных ресурсных центрах в настоящее время занимаются не многие. Образовательные ресурсные центры в большей степени работают с людьми и непосредственно нуждаются в учете всей работы центра. В связи с этим разработка CRM-системы для таких центров является актуальной.

Целью работы является проектирование информационной системы для автоматизации работы образовательного ресурсного центра для вуза.

Разрабатываемая CRM-система для учебного центра должна помочь в решении следующих задач: ведение баз клиентов, моделей, преподавателей и курсов; распределение клиентов по учебным группам и назначение преподавателя; формирование выходных документов (отчетов, списков курсантов и иных печатных форм); уведомления о приближающихся событиях и звонках; сбор статистических сведений по работе менеджеров для дальнейшего анализа. Разрабатываема CRM-система состоит из следующих модулей (рис. 1.):

Модуль «Клиенты». Модуль выполняет функции ведения клиентской базы данных. Первоисточником данных для этого модуля служат входящие звонки. Для каждого клиента заносятся ФИО, список предполагаемых курсов и предпочтительное время занятий, источник из которого была получена информация об учебном центре, контактные данные и дата следующего звонка клиенту. Для прочей информации отведено поле комментариев.

Модуль «Преподаватели». Модуль предназначен для ведения базы преподавателей. На каждого преподавателя заводится отдельная карточка, в которую заносятся ФИО, тип лица (физическое лицо или индивидуальный предприниматель), список преподаваемых курсов и предпочтительное время проведения занятий, статус партнерства и контактные данные. Для записи прочей информации предусмотрено специальное поле. На случай, когда преподаватель

уходит в отпуск, предусмотрена функция деактивации преподавателя, что позволяет исключить его из списков, например, из списка доступных преподавателей (при назначении преподавателя группе).

Рис. 1. Модули CRM-системы

Модуль «Курсы». Выполняет функции для ведения базы преподаваемых в учебном центре курсов. Каждый курс содержит название, краткое описание программы курса, стоимость обучения и учебный центр, в котором проходит обучение.

Модуль «Учебные группы». Для каждого курса существуют отдельные группы, которые делятся по времени обучения. После заключения договора клиент попадает в формирующуюся группу (в зависимости от курса и времени обучения). Группа переходит на обучение когда набирается необходимое количество клиентов, заключивших договора и сделавших первый платеж. Список платежей выводится в виде индикатора, отображающего количество платежей. В момент запуска группы на обучение назначается преподаватель и вводится количество часов обучения и занятий. После запуска группы доступны следующие документы: - договор подряда с преподавателем; - список группы; - приказ о зачислении. При окончании обучения группа закрывается и формируются следующие документы: - приказ о закрытии группы; - акты выполненных работ для слушателей; - акт выполненных работ для преподавателя; - документы об окончании обучения (дипломы).

Модуль «Модели». Предоставляет функции для ведения базы моделей. Каждая модель описывается следующим набором данных: ФИО, контактные данных, возраст и список услуг, на которые модель может быть приглашена. Модели необходимы для обучения парикмахеров, специалистов по визажу, наращиванию ногтей.

Модуль «Расписание занятий». Для создания расписания занятий предусмотрен специальный модуль. Для каждой аудитории составляется недельное расписание. Учебный день условно разбит на три части (утро, день, вечер), для каждой части дня уточняется время и группа занимающихся.

Модуль «Администрирование». Модуль содержит в себе инструменты для управления работой CRM-системы. Модуль включает в себя: инструменты для управления справочниками данных (значения для списков источников информации, типов учебных групп, услуг моделям и т. п.); раздел для загрузки шаблонов документов; логи действия пользователей; список учебных центров; раздел управления пользователями системы, в котором можно добавить пользователей и назначить им соответствующую роль.

Таким образом, разрабатываемая CRM-система представляет собой «клиент-серверное» приложение с трехуровневой архитектурой. В качестве клиентов используются web-браузеры. Причины, выбора «клиент-серверной» архитектуры: - централизованное хранилище данных; - синхронизация серверов после восстановления; - клиенты могут брать данные с разных серверов; - централизованное внесение изменений. В результате внедрения CRM-системы в учебном центре были получены следующие результаты: повышение качества и скорости обслуживания клиентов; сокращение времени на подготовку документов, за счет автоматизации рутинных задач, все документы генерируются автоматически на базе шаблонов загруженных в систему; сокращение времени на обработку заявок клиентов; создана единая база клиентов, преподавателей и моделей, в результате чего сокращено время на поиск необходимой информации; появилось больше времени на поиск потенциальных клиентов; сбор статистики по популярности преподаваемых курсов.

УДК 65.011

Чепоров Валерий Владимирович
к.ф.-м.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

НЕКАЧЕСТВЕННЫЕ ДАННЫЕ В МИС ПРЕДПРИЯТИЙ И ИХ ПОСЛЕДСТВИЯ

Развитие информационных технологий подразумевает, что компании могут хранить все большее количество данных. Однако, работой по обеспечению качества данных часто пренебрегают, в результате чего данные плохого качества являются существенным фактором затрат для многих компаний. Идеальное качество данных не должно быть целью, но вместе с тем, качество данных может быть улучшено только до определенного уровня. Возникает проблема определения оптимального уровня качества данных.

Данные используются во всех видах деятельности компании и составляют основу для решения на разных уровнях. Данные низкого качества могут оказывать значительное негативное воздействие на эффективность организации, в то время как данные высокого качества зачастую являются решающим значением для успеха компании. Тем не менее, несколько опросов отраслевых экспертов показали, что качество данных является областью, в которой многие компании не уделяет достаточного внимания или не знают, как с этой проблемой эффективно бороться.

Некоторые авторы считают, что при классификации данных большинство предприятий имеет дело с тремя категориям данных: мастер-данные, транзакционные данные и исторические данные. Мастер-данные определяются как основные характеристики субъектов предпринимательской деятельности, т.е. клиентов, продуктов, сотрудников, поставщиков и т.д. Транзакционные данные описывают соответствующие события в компании, то есть заказы, счета-фактуры, платежи, поставки, хранение записей и т. д. Поскольку операции базируются на мастер-данных, ошибочные мастер-данные могут привести к значительным издержкам, например, неправильная позиция в цене может приводить к убыткам. В этом контексте некоторые авторы утверждают, что сбор и обработка мастер-данных является деятельностью подверженной ошибкам, когда нарушение архитектуры информационной системы, недостаточная координация с бизнес-процессами, недостаточная реализация программного обеспечения или невнимательное поведение пользователей может привести к разрушению мастер-данных.

С учетом важности наличия правильных и адекватных данных в компании в научной литературе есть общее понимание того, что данные низкого качества является проблемой во многих компаниях. Во многих источниках утверждается, что плохое качество бизнес-данных представляет собой важный фактор затрат для многих компаний, при этом утверждения подкреплены результатами нескольких исследований, проведенных промышленными экспертами.

В литературе можно встретить обобщенные данные о проблемах и последствиях, связанных с качеством данных: 88 % всех проектов интеграции данных полностью или в значительной степени превысили свои бюджеты; 75 % организаций определяли расходы, вытекающие из неочищенных данных; 33 % организаций задерживали или отменяли новые ИТ-системы из-за плохих данных; $611 млрд. в год теряется в США из-за плохо указанных адресов и ошибок вспомогательного персонала в почтовых рассылках; плохие данные стали главной причиной провала CRM систем; менее 50 % компаний утверждают, что очень уверены в качестве своих данных; только 15 процентов компаний уверены в качестве внешних данных, предоставляемые им; данные клиента устаревают на 2 % в месяц, или на 25 % ежегодно; организации обычно переоценивают качество своих данных и занижают цену ошибки.

УДК 338.2

Чепорова Галина Евгеньевна
к.п.н., доцент
Таврический колледж
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАЗВИТИЕ МЕЖФУНКЦИОНАЛЬНЫХ ИНФОРМАЦИОННЫХ КОМПЕТЕНЦИЙ КАК МЕХАНИЗМ СОДЕЙСТВИЯ КОНГРУЭНТНОСТИ ЦЕЛЕЙ ВУЗА

Успешная деятельность любого предприятия основывается на понимании руководством миссии предприятия, разработке и реализации его стратегии на определенную перспективу. После определения целей стратегического уровня необходимо определять цели тактического и оперативного уровня. Важным моментом является понимание всеми членами организации определенных стратегических целей и соответствующих им целей операционного уровня, на котором участниками стратегического процесса являются все сотрудники предприятия.

Процесс подгонки и соответствия операционных целей стратегическим часто называют реализацией принципа конгруэнтности целей. Единственной целью оперативных решений является способствование осуществлению стратегических целей. Таким образом, два уровня являются конгруэнтными, если они служат общей цели.

На наш взгляд, вузы мало отличается от обычного коммерческого предприятия с точки зрения стратегических целей его руководства. Очевидно, что целью руководства вуза является увеличение дохода и снижения затрат. Целью преподавателей является сохранение места работы и повышение своего учебного и научного статуса. При этом интерес преподавателей к стратегии руководства значительно выше, чем такой же интерес работника, например, промышленного предприятия.

Особое место в формировании общности целей внутри организации занимают органы управления вузов в составе департаментов и управлений университета. Многие работники созданной структуры управления в Крымском федеральном университете не имеют опыта работы в соответствующих департаментах и управлениях университета и имеют слабое представление о функциях других подразделений.

Одной и главных проблем современных российских вузов является неэффективная и дорогая система управления. Развитие межфункциональных компетенций сотрудников департаментов университета является одной из ключевых задач формирования стержневых компетенций университета как основы его конкурентных преимуществ, повышения эффективности управления и снижения затрат.

Повышение квалификации может расширить их кругозор, сформировать понимание входных и выходных информационных потоков, что, в конечном итоге, увеличит синергетический эффект системы управления. Выявление и развитие межфункциональных компетенций работников системы управления через программы повышения квалификации может быть реализовано через несколько этапов.

1. Анализ и разработка методик выявления коммуникационных функций департаментов в системе управления вузом.

2. Выявление требований к существующим коммуникационным функциям департаментов университета с точки зрения оценки их автономности, входных и выходных информационных потоков

3. Определение требуемых межфункциональных компетенций сотрудников департаментов

4. Выявление наличия фактических межфункциональных компетенций сотрудников департаментов

5. Формирование интегрированной программы повышения квалификации сотрудников департаментов.

УДК 004.942

Шишкин Владимир Михайлович
к.т.н., доцент,
Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук
Колесников Константин Евгеньевич
студент 5-го курса
Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»
Санкт-Петербург, Россия

ИССЛЕДОВАНИЕ ДИНАМИКИ СИММЕТРИЧНОГО ПРОТИВОБОРСТВА НА ДИФФЕРЕНЦИАЛЬНОЙ МОДЕЛИ

Проблемы информационной безопасности по-прежнему рассматриваются преимущественно с позиций безопасности информации, которая часто сводится к ещё более узкой проблематике - практическим вопросам защиты информации. Для подтверждения этого тезиса достаточно посмотреть перечень специальностей по направлению «Информационная безопасность», в котором преобладает слово «защита».

Никоим образом не умаляя важность и, более того, необходимость повышения качества подготовки специалистов по защите информации с усилением в ней практической составляющей, следует отметить, что такой подход не может обеспечить адекватное реалиям и учитывающее перспективу видение проблем информационной безопасности в их системной сложности.

При этом обратим внимание на следующие аспекты складывающейся ситуации: социо-технический характер угроз и средств обеспечения безопасности, а также тенденцию на то, что обеспечение информационной безопасности на различных её уровнях и в разных аспектах приобретает черты противоборства и становится непрерывным процессом. Ориентация лишь на защиту ресурсов становится недостаточной для поддержания безопасности, технология её обеспечения требует уже тех или иных атакующих или упреждающих воздействий на потенциального противника.

Это обусловлено тотальной информатизацией социо- и техносферы, всех систем обеспечения жизнедеятельности и управления, самого образа жизни подавляющей части населения, перевод конфликтов в информационное пространство. Даже ставший тривиальным сетевой криминал можно интерпретировать как социо-техническое противоборство, а так называемые «информационные войны» глобального уровня вполне могут быть масштабированы до межкорпоративных конфликтов. При этом информационная и материальная составляющие конфликтов стали неразрывно связанными.

Разумеется, обозначенные здесь вопросы активно изучаются, обсуждаются, но, как правило, они сводятся к вербальным рассуждениям, не допускающим объективной оценки. Таким образом, есть потребность в применении формального аппарата, позволяющего если не доказать тот или иной вывод или обосновать рекомендацию, то, по крайней мере, согласовав базовые утверждения модели, объективно проверить результаты экспериментов на ней для различных сценариев и начальных условий.

Ранее нами для исследования взаимодействия развития информационно-коммуникационных технологий и национальной безопасности была разработана математическая модель, показавшая в эксперименте правдоподобное поведение. Она подтвердила возможность применения аппарата обыкновенных дифференциальных уравнений для исследований не только физических или технических объектов, но и для анализа процессов, происходящих в плохо формализуемых системах, не имеющих узко физическую природу. Концептуально эту модель можно отнести к классической традиции, заложенной, в частности, работами Дж.Форрестера или Н.Н.Моисеева в области глобальной динамики.

Далее, в силу отмеченной выше тенденции к противоборству, с целью моделирования динамики информационной борьбы естественным образом появилась новая модель, состоящая из двух симметричных систем замкнутого типа, аналогичных исходной, но взаимодействующих и управляемых. Модель масштабируема, и без изменения структуры, вложив несколько иной содержательный смысл в некоторые фазовые переменные, её можно будет интерпретировать в широком диапазоне от межгосударственного взаимодействия до, например, внутрикорпоративного уровня.

В текущей версии модель представляет собой систему из двенадцати дифференциальных уравнений первого порядка, из которых два описывают динамику использования ресурсов противоборствующих сторон, а остальные десять – фазовых переменных каждой стороны.

Управляющая система, блок управления функционирует самостоятельно. Блок управления состоит из двух элементов «Решающего устройства», в котором содержится вся логика управления, и «Исполнительного устройства», которое выполняет функцию распределения ресурса между потребляющими переменными. Логика управления строится исходя из цели управления и состоит в распределении ресурсов на поддержание уровня соответствующих факторов.

Ресурс понимается в обобщённом, комплексном смысле. Однако в зависимости от назначения и масштаба модели он может пониматься более конкретно, например, как информационный ресурс, хотя и его можно рассматривать в более широком смысле, включая туда не только традиционное содержание, но и обеспечивающие составляющие, например, технологический, энергетический, кадровый, инфраструктурный ресурсы.

Каждое уравнение строится по следующей схеме:

- в левую часть помещается производная данной фазовой переменной;
- правая часть представляет собой линейную комбинацию постоянных коэффициентов, фазовых переменных и их производных, тех, которые влияют на динамику данной переменной (знаки задаются в уравнениях); допускается, что переменная может влиять на свою динамику;
- если на динамику данной переменной влияет ресурс, то в правую часть добавляется ещё одно слагаемое, которое является произведением количества ресурсов на множитель, который показывает долю ресурса, идущего на данную переменную.

В вычислительных экспериментах исследовано поведение такой модели при различных комбинациях стратегических целей (критериев управления) сторон. Определены три принципиально разных варианта целей: подавление, доминирование и паритет. Необходимо отметить, что все эксперименты проводились пока на симметрично настроенной системе, то есть все параметры противоборствующих систем, как и начальные значения фазовых переменных, принимались равными. Но в реальности не существует таких лабораторных условий, поэтому в дальнейших исследованиях целесообразно рассматривать системы с разными настройками, что позволит решать вполне конкретные задачи.

На данном этапе ставилась задача проверки модели, и правдоподобность её поведения подтвердилась. Так, например, система с целью «Паритет» проиграла системе с целью «Подавление», иначе говоря, стратегия «миротворчества» во взаимодействии со стратегией подавления приводит к поражению. Стратегия «Доминирование» требует больших затрат, чем «Паритет», но за счет более интенсивного воздействия на противника через некоторое время использующая её система перестает подвергаться угрозам от противника, и затраты уменьшаются, что эквивалентно выигрышу.

В докладе рассмотрены и проиллюстрированы результаты экспериментов с другими комбинациями стратегий, а также указаны перспективы развития модели и возможности для практического применения.

УДК 004.056.04

Бойченко Олег Валерьевич
д.т.н., профессор,
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Танечник Юлия Сергеевна
курсант 3 курса КФ КрУ МВД РФ
Симферополь, Россия

КИБЕРПРЕСТУПНОСТЬ КАК ПОТЕНЦИАЛЬНАЯ УГРОЗА ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

Введение. В настоящее время современное общество, находится в огромной зависимости от телекоммуникационных и информационных технологий, что приводит нас к росту преступлений в сети интернет. В связи с развитием компьютерных технологий, становится под угрозу безопасность личных данных каждого человека.

Постановка проблемы. Внедрение новый информационно коммуникационных технологий, привело к появлению новых видов преступлений, так называемых «киберпреступлений», которые направлены на утечку личных данных, вмешательство в работу электронно-вычислительных систем, хищение информации, то есть действия, которые носят противоправный общественно опасный характер, они совершаются с помощью компьютеров, компьютерных сетей и программ.

Целью данного исследования является, изучение «киберпреступности», как потенциальной угрозы информационному обществу и методов борьбы с ней, а так же рассмотреть нормативно правовые акты, которые регулируют отношения в сфере информационных технологий, в сфере компьютерной информации.

Методы исследования. Защита информационной безопасности, является огромным приоритетом государства, так как преступность в виртуальном пространстве с каждым днем все сильнее набирает обороты. «Киберпреступлениям», могут быть подвергнуты не только люди, но и целые государства, так как «киберпреступность» не имеет государственных границ.

Непосредственно рост киберпреступности, негативным образом сказывается на современном обществе, так как с развитием и появлением новых технологий, все больше страдает безопасность данных людей. На данный момент общество все больше и больше пользуется электронными технологиями и иными нововведениями, так например большинство людей, пользуется электронными кошельками, оплачивают свои услуги через сети интернет, что делает их личные данные более доступными для злоумышленников, которых на данный момент становиться все больше в сети интернет.

Для того, что бы определить методы борьбы с «киберпреступностью», необходимо начать с самого понятия, а так же рассмотреть типы компьютерных преступлений .

Итак, важным шагом в борьбе с «киберпреступлениями», было принятие Советом Европы Конвенции «по борьбе с киберпреступностью» от 23 ноября 2001 года. Согласно данной Конвенции «киберпреступность - это правонарушения, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных»

Конвенция выделяет четыре типа компьютерных преступлений:

- незаконный доступ – ст.2;
- незаконный перехват – ст.3;
- вмешательство в данные – ст.4;
- вмешательство в систему – ст.5.

В Уголовном кодексе Российской Федерации существует ст. 159.6, которая предусматривает уголовную ответственность за мошенничество в сфере компьютерной информации. Данное деяние может быть совершенно, исключительно с использованием современных компьютерных технологий. Противоправные общественно опасные деяния в сфере электронной техники, а так же информационных технологий, выражается в том, что они могут повлечь за собой нарушение контроля различных объектов, создать серьезные проблемы работы ЭВМ, исказить либо копировать информацию с информационных ресурсов, которые могут нанести значительный ущерб.

В законодательстве Российской Федерации существует, Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017). Данный закон регулирует общественные

отношения в сфере обеспечения защиты информации, применении информационных технологий, а так же осуществление права на поиск, получение, передачу, производство и распространение информации.

Исходя из этих нормативно правовых актов, можно сделать вывод, что внутренние законодательство Российской Федерации, напрямую не предусматривает и не регулирует ответственность за «киберпреступления», а лишь косвенным образом предусматривают ответственность, в сфере компьютерной информации и обеспечения защиты информации.

Тем самым внутреннее законодательство Российской Федерации не закрепляет понятия «киберпреступность», и напрямую не предусматривает ответственность за совершение «киберпреступлений», но регулирует, некоторые общественные отношения входящие в понятие «киберпреступность».

Результаты исследования. К методам борьбы с «киберпреступностью», можно отнести, непосредственно, то что необходимо повышать свою грамотность в пользовании сети интернет, то есть не скачивать с подозрительных сайтов программы, не скачивать непонятные сообщения, которые поступают на электронную почту, а так же как можно меньше выкладывать своих личных данных в сети интернет.

К следующим методу борьбы, можно отнести «автоматическое обновление», данный метод поможет обезопасить личные данные и повысит уровень безопасности ПО компьютера. Как метод защиты следует рассматривать, так же «облачные» технологии, которые в свою очередь помогают защитить информацию от заражения и утечки.

Так же, что бы уменьшить количество «киберпреступлений», необходимо усиление в сфере международного сотрудничества Российской Федерации и иных государств, так как многие злоумышленники, которые совершают преступления против Российской Федерации, находятся за пределами нашего государства.

Выводы. Для эффективной борьбы с «киберпреступностью» необходимо вводить нормы непосредственно, как внутригосударственные, которые будут регулировать напрямую борьбу с «киберпреступностью», а не только некоторые отдельные общественные отношения, которые, только частично затрагивают «киберпреступность». Но, так же необходимо введение международных норм, которые будут предусматривать, международную ответственность за «киберпреступность», то есть повышать уровень эффективной борьбы с данными преступлениями, между государствами.

Чем подробнее будет прописана норма, предписывающая запрет на совершение противоправных общественно опасных деяний в сфере «киберпреступности», тем эффективнее будут данные методы борьбы с преступностью в данной сфер.

УДК 347.1+343

Журавленко Николай Иванович
к.ю.н., доцент,
Крымский филиал Краснодарского
университета МВД России
Республика Крым, Россия

ЗАЩИТА ОТ УГРОЗ ЭКОНОМИЧЕСКОЙ РАЗВЕДКИ ЗА РУБЕЖОМ

История экономической разведки так же стара, как и история экономических отношений. Борясь за рынки сбыта древние купцы (в том числе и российские) любопытствовали, какой товар, в каком количестве и какого качества привезли на данный рынок конкуренты, по какой цене они намерены его продавать. При этом они не упускали возможность пустить слух о том, что товар ворованный, низкого качества и стоит непомерно дорого. Позднее эти приемы получили названия: коммерческий шпионаж, диффамация, компроментация. Недобросовестная конкуренция осуществляется также и с помощью подкупа, коррупции, ложной рекламы, подделки продукции конкурента, демпинга цен и экономической разведки.

В противовес промышленному и экономическому шпионажу владельцы производственных и коммерческих секретов всегда тщательно охраняли их от конкурентов. Например, охота европейцев за секретом китайского фарфора, открытого еще в IV в., продолжалась длительное время и не принесла положительных результатов, пока в начале XVIII в. не был изобретен способ производства фарфора в самой Европе. Еще более древним предметом охоты промышленных шпионов был шелк.

Характерной чертой современной экономической политики развитых стран является дальнейшее сплочение государственных и негосударственных структур для продвижения товаров своих производителей на мировых рынках. В ее реализации участвуют спецслужбы и частные детективные фирмы, нередко использующие подкуп, шпионаж, дезинформацию и другие неблаговидные приемы.

По подсчетам специалистов, только в США ежегодные затраты частных фирм на цели экономической разведки превышают 1,5 миллиарда долларов. Японские корпорации получают таким путем 40 % информации о технических достижениях европейцев и американцев. Охота за промышленными секретами позволяет компаниям сэкономить собственные средства на ведение фундаментальных исследований и конструкторских работ, использовать научно-технические достижения конкурентов, сосредоточив все внимание на производстве и маркетинге.

Наиболее результативно экономической разведкой занимаются крупные концерны и транснациональные компании. Существуют даже тайные процветающие биржи, где продают краденые промышленные секреты: в Японии – по электронике и пластмассам, в Италии – по фармацевтике. Экономическая разведка не знает границ – «черные биржи» имеют своих коммивояжеров, которые разъезжают по всему миру, покупая и продавая коммерческую информацию. Они располагают достоверной информацией о финансовых и торговых возможностях компаний, их контрактах и дальнейших планах, о перспективных разработках и готовящихся к серийному выпуску товарах.

Крупные фирмы имеют разведывательные подразделения, иногда коммерческий шпионаж осуществляют их службы безопасности. Кроме собственных служб, корпорации активно используют и услуги самостоятельных фирм, специализирующихся на работе с экономической информацией. Одна из таких компаний располагает штатом в 20 тысяч сотрудников и имеет 22 отделения в США, а также филиалы в Англии, Франции, Италии и странах Латинской Америки. Ее постоянными клиентами являются 3 тысячи американских компаний.

В связи с огромной опасностью для коммерческих структур, которая исходит от экономического и промышленного шпионажа, особый интерес представляет опыт нормативного урегулирования вопросов защиты коммерческой информации за рубежом. За многовековую историю развития капитализма в западных государствах выработана разветвленная система правовых актов, обеспечивающих защиту коммерческих секретов от недобросовестных конкурентов. В большинстве стран защита коммерческой информации обеспечивается самими фирмами, а не государственными органами.

В США согласно Закону о коммерческой тайне или по принятой там терминологии – «фирменных секретах» («секретах производства»), принятому в 1979 году, коммерческой тайной является информация, которая имеет самостоятельную экономическую стоимость вследствие того, что она не является общеизвестной или доступной лицам, которые могут ее использовать в коммерческих целях, а также если она является объектом разумных усилий по защите.

Фирмы, покушающиеся на чужую интеллектуальную собственность, платят в этой стране штрафы, исчисляющиеся сотнями миллионов долларов. Так, федеральный суд США обязал компанию, незаконно использовавшую разработку другой фирмы, выплатить последней 116 миллионов долларов компенсации за нанесенный ущерб.

В ФРГ действует закон о недобросовестной конкуренции, в соответствии с которым к коммерческой тайне отнесены: коммерческие замыслы и цели фирмы, размеры и условия банковских кредитов, балансы и бухгалтерские книги, негласные компаньоны товариществ, компьютерные программы, картотеки клиентов и т.д. При этом ответственность за разглашение коммерческой тайны несут не только сотрудники фирмы, которым были доверены или стали известны производственные секреты фирмы, но и третьи лица.

Для Франции характерно определение должностей лиц, имеющих доступ к тайне предпринимательства. Физическое лицо становится носителем профессиональных секретов в силу занимаемой им должности, положения или в результате выполнения порученной ему функции постоянного или временного характера.

В Японии нет ни законов, ни каких-либо других нормативных документов, предусматривающих ответственность за разглашение коммерческой тайны, а действуют только акты (кодексы) фирм. Специалисты утверждают, что японский бизнес менее всего страдает от утечки информации, поскольку основан на системе пожизненного найма и воспитания у сотрудников чувства патернализма, когда они считают себя членами одной семьи, родителями в которой являются руководители фирмы.

В европейской практике можно проследить известную степень беспечности предпринимателей, основанную на их твердом убеждении, что конкуренты не должны

использовать «неджентельменские» методы. Идея западного торгового права о безоговорочной порядочности предпринимателей основана на убежденности в исключительной добросовестности предпринимателей в соответствии с негласным «моральным кодексом» (morality Kodex).

Установление правовых основ защиты коммерческой тайны является важным элементом юридического обеспечения предпринимательской деятельности. В большинстве экономически развитых зарубежных стран законодательство, регулирующее правовой режим коммерческой тайны и устанавливающее ответственность за ее неправомерное использование, представляет собой весьма развитый нормативный массив, формирование которого осуществляется как на основе национальных правовых традиций, так и в соответствии с современными стандартами международной торговли.

УДК [338.46 : 007] : 005.922.1

Смирнова Оксана Юрьевна,
ассистент
Институт экономики и управления,
Смирнова А. Ю.
студентка кафедры физики твердого тела,
Физико-технический институт,
ФГАОУ ВО КФУ им. В.И.Вернадского,
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ИНДУСТРИИ ИНФОРМАЦИОННЫХ УСЛУГ ТУРИСТИЧЕСКОГО БИЗНЕСА

Информационное пространство и соответственно информационная безопасность подвергается угрозам ежесекундно. Туристическая отрасль является наиболее чувствительной, так как туристические компании обрабатывают различную информацию клиентов, являющейся конфиденциальной. Индустрия туристических услуг чаще всего использует оплату по сети интернет:

- сервис бронирования номеров в отелях, гостиницах;
- резервирование авиабилетов,
- резервирование билетов экскурсионных маршрутов;
- сервис бронирования и резервирования столиков в кафе, ресторанах;
- другой инфраструктуры в сфере путешествий и туризма.

Информационная безопасность туристической фирмы может быть обеспечена только при условии строгого соблюдения норм в области защиты персональных данных. Поэтому, для индустрии информационных услуг в туристической сфере первостепенной задачей является безопасная обработка банковских данных и реализация всех требований PCI DSS. Стандарт PCI DSS (Payment Card Industry Data Security Standard) создан для обеспечения безопасности обработки, хранения и передачи информационных данных о пользователях платежных карт, международных платежных системам Visa, MasterCard и т.д.

Информационная безопасность любой фирмы, в том числе и туристической – база методов и средств, которые обеспечивают защиту корпоративной информации, ее конфиденциальность, целостность, доступность, достоверность, аутентичность, в условиях воздействия на нее угроз всевозможного характера.

На сегодняшний день туристические фирмы сталкиваются с различными угрозами информационной безопасности от внутренних и внешних источников:

- хакеры и вредоносные программы;
- инсайдеры;
- незлонамеренные нарушители;
- форс-мажоры (стихийное бедствие, пожар, авария в энергосистеме и т.д.).

Атаки киберпреступности на информационные системы туристических фирм преследуют следующие цели:

- финансовая информация и эксплуатация ресурсов корпоративной сети,
- ограничение деятельности фирмы,
- прекращение взаимоотношений с партнерами по бизнесу и т.д.

Виды угроз информационной безопасности:

– вредоносные программы и аппаратные и программные закладки,
– спам-рассылки,
– устройства для перехвата сигналов связи и др.

Следовательно, система защиты информации должна предотвращать:

– утечку, хищения, утраты, искажение, контрафакцию информации;
– несанкционированные действия по уничтожению, модификации, искажению, копированию, блокированию информации;
– другие формы незаконного проникновения в информационные ресурсы и системы;
– создание резервных копий, послеаварийное восстановление информационных систем и т.д.

Как правило, информационная безопасность сферы индустрии информационных услуг туристического бизнеса обеспечивается стандартными процедурами, средствами, координационными и техническими мерами высокого уровня чувствительности, которые способствуют защите данных. Координационные меры заключаются в правилах работы с различными видами информации, ИТ-сервисами, средствами защиты и т.д., а также в документировании процедуры защиты данных.

Технические меры могут быть реализованы:

– в криптографических средствах (шифрование, цифровая подпись), средствах защиты от несанкционированного доступа, предотвращения взлома;
– в системах анализа и моделирования информационных потоков (CASE-системы), системах аутентификации (пароль, сертификат, биометрия), мониторинга сетей и резервного копирования.

Следовательно, создать условия для информационной безопасности фирмы возможно только при целостном и планомерном подходе к средствам защиты. Своевременные средства защиты - залог информационной безопасности. Система ИБ должна учитывать все современные компьютерные угрозы и уязвимости и осуществлять непрерывный контроль в реальном времени всех событий, влияющих на безопасность данных. Защита должна реализовываться в режиме «нон стоп» и распространяться на весь жизненный цикл информации - от ее создания до удаления или потери актуальности.

УДК 004.056

Бойченко Олег Валерьевич
д.т.н., профессор,
Броцкая Лолита Олеговна
студентка 4 курса бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СОЗДАНИЕ И РАЗРАБОТКА ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

На данный момент автоматизированные информационные системы (АИС) рассматривают как необходимую часть инфраструктуры бизнеса.

Например, в странах с развитой экономикой, данные системы применяются как инструмент решения задач управления предприятием.

Приведем примеры таких задач.

1. Планирование производственной деятельности информационной системы управления предприятием (ИСУП) осуществляет поддержку решения задач создания производственных планов, а также проверку возможности исполнения данных планов при имеющихся ресурсов.
2. С помощью ИСУП управление финансовыми ресурсами предприятия осуществляется более эффективно, за счет составления прогнозов движения денежных средств, которые позволяют своевременно предвидеть сроки возможного наступления недостатка денежных средств для уплаты срочных долгов.
3. За счет ИСУП более эффективно осуществляется управление затратами предприятия. Обеспечивается путем максимальной детализации учета всех затрат предприятия и увеличения оперативности калькуляции себестоимости готовой продукции и услуг.

Решение перечисленных выше задач возможно только тогда, когда все подсистемы ИСУП интегрированы и соответствующее программное обеспечение (ПО) поддерживает современные компьютерно-ориентированные технологии управления.

Создание эффективной ИСУП позволяет оперативно обрабатывать и готовить различную сопровождающую документацию. Это позволяет обслужить большое количество клиентов, не заставляя их ждать.

Современная ИСУП должна интегрировать все информационные потоки предприятия при этом обеспечивать персонал всей необходимой информацией для принятия управленческих решений.

Создание и разработка ИСУП, в принципе, как и других автоматизированных систем, начинается со сбора и анализа информации о функциях, процессах и структуре предприятия.

Основным при разработке ИСУП является выполнение комплексного анализа, который требует использование разных типов моделей, которые отображают различные стороны деятельности системы. Поэтому от выбора инструментальных средств моделирования очень зависят объем и сроки выполнения работ, качество анализа при создании проекта ИСУП.

В процессе разработки ИСУП осуществляются три уровня анализа, которые соответствуют трем стадиям создания ИСУП.

Первым уровнем является определение требований. Данная стадия начинается со сбора информации об исходной системе. Затем собранная информация отображается в виде моделей текущего состояния объекта проектирования. Далее осуществляется создание концептуальных моделей будущей ИСУП. Здесь происходит совмещение знаний о предметной области со знаниями об объекте проектирования, которые представлены в виде моделей текущего состояния. Итогом данного уровня чаще всего является техническое задание (ТЗ) на ИСУП.

Второй уровень – это формирование спецификаций, которое сопровождается выпуском проекта ИСУП. На этом этапе в основном принимаются во внимание ограничения, которые надо учесть в моделях ИСУП.

Третьим уровнем является непосредственно само внедрение. Данный уровень связан с конкретной реализацией проекта ИСУП на предприятии.

При выполнении процессов по моделирования на данных уровнях используются различные инструментальные средства.

Инструментальные средства классифицируют в зависимости от класса создаваемой ИСУП. Итак, инструментальные средства для моделирования информационных систем относятся к следующим категориям.

Первая категория инструментальных средств это локальные, которые поддерживают один и два типа моделей и методов, например, ProCap, CASE Аналитик. При разработке ИСУП такие средства используются только на концептуальном уровне для предварительного анализа. С помощью локальных средств задача комплексного анализа системы не решается.

Следующей категорией являются малые интегрированные средства моделирования, например, Erwin, BPwin. Также как и локальные, малые средства изначально не предназначены для комплексного анализа систем. За счет них можно разрабатывать локальные ИСУП или небольшие подсистемы, которые предназначены для автоматизации отдельных бизнес-цепочек. Особенностями данной категории являются наличие независимых компонентов и интеграция моделей за счет экспорта и импорта данных.

Третьей категорией являются средние интегрированные средства моделирования, которые поддерживают от 4 до 15 типов моделей и методов, например, Rational Rose, Paradigm Plus. Данная категория представляется программными продуктами, при создании которых первоначально заложены требования комплексного использования различных методов и типов моделей. Такая категория предназначена для комплексного анализа систем, которая может быть успешно использована при создании малых и средних ИСУП. Но в данных средствах есть и отрицательный момент – это недостаточные возможности для моделирования и анализа требований.

Последняя категория – это крупные интегрированные средства моделирования, которые поддерживают более 15 типов моделей и методов, например, ARIS Toolset. Такие системы предназначены для проектирования крупных ИСУП, например, системы управления предприятием типа ERP.

В результате можно сделать вывод, что от использования ИСУП наблюдается эффект, который можно представить в следующих результатах:

1. Формирование общей базы информации обо всех сторонах деятельности предприятия;
2. Значительно снижаются затраты на контроль деятельности сотрудников;
3. Упорядочивается управление процессами предприятия, в любое время можно увидеть текущее состояние любого процесса и результаты деятельности предприятия;
4. Уменьшается себестоимость товаров и услуг, которые производит предприятие;
5. За счет ускорения процессов предприятия увеличивается денежный поток от бизнес-деятельности предприятия.

УДК 004.056.5

Бойченко Олег Валерьевич
д.т.н., профессор
Панченко Игорь Александрович
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

На современном этапе развития информационных технологий все большую популярность набирает развитие так называемых «облачных сервисов», которые предлагают своим клиентам получить выгоду от внедрения, обеспечить максимальный уровень безопасности и доступности программных комплексов и хранении информации.

При этом угрозы информационной безопасности совершенствуются с каждым днем, и у каждого из сервисов существуют свои особенности защиты. У облачных сервисов, за счет использования различных технологий и моделей существуют свои особенности обеспечения безопасности клиентов.

Облачные технологии это модель онлайн хранилища и предоставления сервисов в которой данные хранятся на большом количестве серверов, предоставляемых пользователям «облачных услуг».

Особую популярность распространение облачных технологий получили среди крупного бизнеса, который медленно и уверенно переводит свою деятельность в облачные сервисы.

Исходя из исследований, которые провели аналитики Orange Business Services, рост рынка облачных сервисов в России с 2012 по 2016 г. вырос почти в четыре раза и составил около 19 млрд р.

Рис. 1. Объем российского рынка облачных услуг

Как отмечают аналитики: «Предполагается, что рынок услуг, основанный на построении облачной инфраструктуры, развиваясь также активно, к 2016 г. превысит объем рынка самих облачных услуг.

Это станет возможным благодаря стремительному росту объема услуг по строительству «облаков», их слиянию и кастомизации, а также перемещению с привычной инфраструктуры на облачную. Всего к 2016 г. доля облачных услуг должна достичь 13 % от всего российского рынка IT-сервисов (рис. 1)».

Главным аспектом, которому уделяется особое внимание при переходе к облачным технологиям, является информационная безопасность. Многие компании до сих пор не торопятся внедрять облачные технологии ввиду многих причин безопасности. Не стоит забывать, что облачный сервер - это тот же сервер что и на предприятии, только расположенный за его пределами, таким образом, угрозы безопасности которым подвержено стандартное программное обеспечение и хранилища данных подвержены и облачные серверы.

Однако, существуют и специфические, характерные только для облачных серверов, угрозы безопасности, наиболее актуальными из которых являются следующие:

- уязвимости, связанные с потерей и утечкой данных актуальны в связи с тем, что при выборе облака не существует физического доступа к инфраструктуре данных и программного обеспечения. Наибольшая вероятность потери или перехвата ваших данных возникает при передаче или приеме информации через каналы Интернет. В этом вопросе особое внимание стоит уделить шифрованию данных передаваемых через каналы связи, так как шифрование дает возможность сохранить и обеспечить безопасность на всем пути следования информации;

- уязвимости API - интерфейсов прикладного программирования, которые используют поставщики облачных сервисов для доступа к управлению и мониторингу. Он позволяет обеспечить мониторинг доступа к сервисам, так же выявить случаи несанкционированного доступа и активности. В решении этих проблем поможет использование шифрования, каналов аутентификации и проверки пользователей;

- похищение данных учетных записей пользователей облачных сервисов. Развитие программ шпионов и так называемых программ «угонщиков» паролей заставляет серьезно задуматься о потере учетных записей. Основное бремя защиты от такого типа угроз в большей степени ложится на пользователей облачными сервисами, чем на поставщиков. Поэтому каждый из пользователей облачными ресурсами должен не только позаботиться о корпоративной безопасности, но и о безопасности своего устройства, с которого он получает доступ к облачному сервису. В этом на помощь придут антивирусные программы, брандмауэры и прочее антивирусное программное обеспечение. Так же одним из эффективных способов защиты от такого рода угроз является двухфакторная аутентификация, которая получает все большее распространение;

- действия инсайдеров являются самым распространенным и незащищенным каналом утечки информации. Отличительной чертой облачных технологий в данном случае является отсутствие у покупателя какой-либо информации сотрудниках компании поставщика, возможности проверки и контроля, принципов и методов приема на работу. С другой стороны, каждая серьезная компания намерена сохранить свое имя и должным образом проводить подбор персонала и случаи утечки информации. Так же стоит обратить внимание на скорость реакции и принятия мер поставщиком в случаях утечки информации при действии инсайдеров.

Большинство угроз, с которыми сталкиваются «облачные технологии», схожи с угрозами безопасности корпоративного сегмента, поэтому при переходе в облако принципы и методы защиты сходны с корпоративной защитой.

Сталкиваясь с особенностями безопасности облачных вычислений, не стоит забывать о том, что внедрение новых разработок всегда сопряжено с определенной долей рисков. Учитывая то, что внедрение и переход к использованию облачных сервисов сопряжен с определенными рисками, можно с уверенностью утверждать, что стремительное развитие технологий безопасности и облачных сервисов позволит свести к минимуму риски связанные с защитой данных в облаке.

УДК 65.011

Бойченко Олег Валерьевич
д.т.н., профессор,
Федосеева Карина Николаевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Актуальность работы. В наше время доминирующее место среди инструментов хранения больших объемов информации заняли системы управления базами данных (СУБД), в частности реляционные. Развитые информационные приложения опираются на многопользовательские СУБД, работающие по технологии клиент/сервер.

В таком сочетании обеспечение информационной безопасности СУБД и ее серверных составляющих, несет важное значение для безопасности организации в целом.

Целью работы является анализ существующих проблем и методов обеспечения информационной безопасности (ИБ) систем управления БД.

Для СУБД важными являются три основных аспекта ИБ: доступность, целостность и конфиденциальность. В связи с этим СУБД имеет свои привилегии которые можно подразделить на две категории: привилегии безопасности и привилегии доступа. Благодаря привилегиям безопасности появляется возможность выполнять административные действия.

Именно привилегии доступа, позволяют определять права доступа субъектов к определенным объектам.

Система управления БД имеет специальное средство управления доступом, а именно средство представления данных, позволяющее делать для субъектов видимыми определенные столбцы таблиц или отбрить некоторые строки.

Таким образом, создавая правильные представления и не давая субъектам все права доступа к базовым таблицам, администратор БД защищает таблицы от неразрешенного доступа, при этом каждый пользователь получает виденье базы данных, в которой недоступные объекты не фигурируют.

Некоторые средства управления доступом, и определенные операторы СУБД позволяют осуществлять следующие виды ограничения доступа: ограничения по операциям, ограничения по значениям, ограничения по ресурсам.

Для коммерческих организаций гарантирование целостности информации и данных является не менее важно, чем обеспечение конфиденциальности.

Одной из главных проблем баз данных является ошибки, осуществляемые оборудованием, администраторами, пользователями и прикладными программами. С точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются ограничения и правила.

Главный источник угроз, присущих системе управления, заключается в природе самой базы данных. SQL является основным средством взаимодействия с СУБД. Это важный непроцедурный инструмент для определения и управления данными.

Механизм, включающий в себя некоторые правила, дает возможность конструировать сложные для анализа цепочки действий, при этом пользователю передается право на выполнение процедур, даже если он не имеет на это полномочий. В результате этих действий пользователь, который может являться злоумышленником, получает удобный и мощный инструмент, который может менять структуру БД.

Существует несколько угроз, возникающих при использовании злоумышленником средств языка SQL, наиболее известными из которых являются следующие:

1) Получение информации путем логических выводов

Довольно часто путем логического вывода из базы данных извлекается информация, на получение которой стандартными средствами у пользователя не хватает привилегий. При использовании представлений для реализации контроля доступа, если они допускают модификацию, с помощью такой операции можно получить информацию о содержимом базы данных.

Тщательное проектирование модели данных, является основным средством борьбы с такого рода угрозами, однако помимо этого способа эффективным является также механизм размножения строк. Суть этого метода заключается в том, что состав первичного ключа, внедряется метка безопасности, и за счет нее возникает возможность хранить в таблице некоторое количество экземпляров строк с идентичными значениями ключевых полей.

2) Агрегирование данных.

Агрегированием называется способ получения новой информации, используя комбинирование данных, полученных законным образом из различных таблиц.

3) Покушения на высокую доступность.

Доступ пользователя ко всем возможностям SQL, может привести к затруднению работы других пользователей.

В качестве любопытной угрозы, специфичной для реляционных СУБД, упомянем ссылочные ограничения.

Строго говоря, наложение такого ограничения препятствует удалению строк из таблицы, содержащей первичные ключи, хотя в современных версиях SQL можно запросить так называемое каскадное удаление. Впрочем, искажение прочих ограничений на таблицы и их столбцы по-прежнему остается опасным средством покушения на доступность данных.

Защита коммуникаций между сервером и клиентами. Проблема защиты коммуникаций между сервером и клиентами не присуща СУБД, она является специфичной для всех распределенных систем.

Однако такова проблема возникает и при работе с системой управления. Для решения таких проблем используются общие методы, к примеру, такие же как в распределенной вычислительной среде. Для этого разработчики СУБД погружают свои программные продукты в вычислительную среду.

Администратор может задать один из пяти существующих уровней защиты для каждого приложения клиент-сервер:

- защита пересылаемой информации при осуществлении соединения клиента с сервером;
- защита персональных данных только на начальном уровне реализации удаленного вызова процедуры (в момент получения сервером первого запроса);
- подтверждение достоверности источника данных (проверка, поступающих на сервер данных, на принадлежность определенному клиенту);
- подтверждение истинности источника и целостности данных (проверка данных на изменения);
- подтверждение конфиденциальности и целостности данных (проверка данных на изменения и осуществление шифрования всех пересылаемых данных).

Обеспечение информационной безопасности БД сложная задача, т.к. конфигурация, в которую имеет доступ хотя бы один из программистов, не может считаться безопасной.

Не считая регулярного применения всех этих методов и средств необходимо также использование административных и процедурных мер. В таком случае можно рассчитывать на нужный результат в обеспечении информационной безопасности современных серверов баз данных.

УДК 681.5.03

Дячук Виктория Сергеевна,
аспирант
Антропова Анна Александровна
студент 3-го курса
Таратухина Татьяна Сергеевна
студент 3-го курса
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

КРИТЕРИИ АНАЛИЗА ИНТЕРФЕЙСА АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОММЕРЧЕСКОГО УЧЕТА ЭЛЕКТРОЭНЕРГИИ

В условиях развития современного общества возрастает роль автоматизации информационного обмена для обеспечения полноценной жизни человека и его взаимодействия с окружающей средой. Процесс автоматизации как метод обеспечения информационной безопасности занимает спорную позицию, однако его эффективность по части минимизации человеческого фактора и его влияния на сохранность данных достаточно велика. Согласно данным исследования The Global State of Information Security Survey 2016 в 2015 году количество выявленных инцидентов в сфере информационной безопасности выросло на 38%. При этом, главными источниками ИБ-инцидентов определены сотрудники компаний и организаций: действующие - 34%, а также бывшие - 29%. Следовательно, при такой высокой вероятности риска потерь за счет человеческого фактора, весомым и необходимым является обеспечение персонала удобством работы с автоматизированным программным обеспечением. Здесь на первый план выступает такая характеристика систем как юзабилити интерфейса.

Интерфейс можно характеризовать как некий «мост» между пользователем и системой, с помощью которого специалист может объяснить системе, чего он от неё хочет, а система это выполнит. Юзабилити (от англ. usability — дословно «возможность использования», «способность быть использованным», «полезность») интерфейса определяет его удобство для пользователя в контексте достижения поставленной им цели. (формирование отчетности, импорт и экспорт данных, заполнение базы данных, вывод данных на печать и т.д.).

Для анализа юзабилити интерфейсов мы выбрали программные комплексы (далее – ПК) автоматизированных систем коммерческого учета электроэнергии как объекта критической инфраструктуры. Среди популярных и доступных к обзору ПО АСКУЭ мы выделили:

1) «Учет энергоресурсов» НПО «МИР»;
2) «АльфаЦЕНТР Standard edition» от компании Эльстер Метроника;
3) Система ЛЭРС УЧЕТ.

С учетом специфики вышеуказанных программных комплексов были определены следующие критерии для анализа юзабилити интерфейса:

1. Быть интуитивно понятным:

а) все элементы выстроены по принципам элементарной логики;

б) кнопкам присвоены понятные обозначения;

в) есть помощь пользователю, если он “заблудился”.

2. Быть предсказуемым: каждый элемент интерфейса соответствует своему визуальному отображению.

3. Быть минималистическим: лаконичный интерфейс, не содержит ничего лишнего – только необходимое по делу.

4. Быстро загружаться: реагирование программы на клик пользователя не должно превышать 3 секунд.

5. Показывать все важные опции: наиболее вероятные и часто выполняемые действия пользователем должны находиться на «открытом» месте, в то время как второстепенные функции могут быть вызваны контекстным меню.

6. Уметь общаться с пользователем: вывод на экран пользователя сообщения с наименованием выполняемого в данный момент процесса.

7. Иметь разные стили для кнопок с разными типами действий:

а) кликабельные и некликабельные элементы должны быть различны;

б) выделение цветом или стилем тот раздел меню, в котором в данный момент находится пользователь.

8. Быть привлекательным: иконки и объемность изображения, цветовое решение и расположение элементов.

9. Давать возможность персонализации: настройка интерфейса «под себя» - возможность увеличить шрифт, изменить иконку пользователя и т.д.

10. Быть лояльным к ошибкам пользователя: функции возврата и предотвращения ошибочного действия.

11. Говорить на языке пользователя: язык интерфейса должен быть настроен на целевую аудиторию.

12. Предоставлять оптимальное количество вариантов выбора: количество вариантов возможных действий для пользователя не должно быть слишком велико, чтобы не отвлекать внимание пользователя от основной работы в системе.

13. Давать мягкие подсказки: текст подсказок должен быть обращен к пользователю и содержать информации из руководства подльзователя.

14. Выделять модальное окно: затемнять фон под активным модальным окном, пока пользователь не выполнит в нем действие.

15. Иметь короткие формы регистрации: для отправки документации пользователю достаточно ввести свои авторизационные данные (логин и пароль)

16. Иметь простые принципы заполнения полей: поле должно заполняться сразу после клика на него; поле с автозаполнением (выбор из выпадающего списка, автозаполнение текущей даты и т.д.).

17. Предоставлять варианты удобного управления: управление мышью и клавиатурой в комплексе или отдельно на выбор пользователя.

Таким образом, при следовании всем вышеупомянутым критериям юзабилити интерфейса, пользователь программного обеспечения автоматизированной системы коммерческого учета электроэнергии минимизирует риск несанкционированного нарушения защиты данных, тем самым повышая уровень информационной безопасности в системе.

УДК 004.056.53

Мокрицкий Вадим Андреевич
старший преподаватель
Таратухина Татьяна Сергеевна
студентка
Антропова Анна Александровна
студентка
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ ДАННЫХ В СУБД

В последнее время количество случаев хищения персональных данных значительно возросло в связи с утечкой информации из баз данных и различными махинациями с информацией, хранящейся в БД больших организаций. Информация является очень дорогим и важным ресурсом, а следовательно базы данных регулярно подвергаются нападениям злоумышленников.

Большинство случаев кражи информации осуществляются легальными пользователями через бреши в информационной безопасности компании, и уязвимостей СУБД в частности. Все эти случаи стали причиной пересмотра требований не только к усовершенствованию информационной безопасности внутри компаний, так и к пересмотру требований регуляторов к обеспечению защиты данных. Почти все регуляторы (Федеральный закон «О защите персональных данных», PCI DSS, HIPAA, SOX и т.д.) указывают на необходимость постоянного контроля доступа к информации, поиск уязвимостей в системе, а так же обеспечение защиты данных при их передаче. Отдельное внимание уделяется контролю за привилегированными пользователями, и контролю доступов к данным пользователей бизнес-приложений таких компаний, как Oracle, PeopleSoft, SAP, и приложений собственной разработки, поскольку это является одной из главных угроз хищения данных.

Одним из способов защиты данных является мониторинг средствами СУБД и приложений. Почти все основные разработчики СУБД попытались встроить средства контроля, однако это привело к ряду недостатков. Средства СУБДТ не имеют возможности точно отличить

злоумышленника от пользователя, использование таких средств приводит к сильному увеличению нагрузки на серверы, вследствие чего значительно ухудшается производительность и качество программ.

Обычно оптимизация производительности программ осуществляется благодаря методу "connection pooling", который подразумевает использование единой учетной записи для доступа к БД. Этот метод не показывает имена конечных пользователей программ, осуществляющих доступ к базе данных, т.е. становится невозможной идентификация конечного пользователя программы, запросившего сделавшего запрос информации. Данный метод имеет ряд преимуществ, среди которых повышение производительности программ, уменьшение нагрузки на СУБД, однако при это уровень информационной безопасности снижается, потому что нет возможности контролировать работу конечных пользователей.

В идеале, необходимо найти такое решение, которое бы контролировало движение информационных потоков и при этом не сказывалось на производительности приложений. Это привело к появлению класса DAM (Database Activity Monitoring), который контролирует всю активность на серверах управлении БД, WAF (Web Application Firewall) для контроля за доступом и управлением базами данных и DLP (Data Leak Prevention) для контроля за движением информации.

Так же для обеспечения информационной безопасности данных используются межсетевые экраны Web-приложений (WAF). Обычно это программно-аппаратные комплексы, использующие наборы правил и политик безопасности к наблюдаемому HTTP-трафику, идущему от приложений к БД и в обратную сторону. Они дают возможность контролировать такие виды атак, как Cross-site Scripting (XSS) или SQL-инъекции. При настройке правил под конкретную программу, можно найти и блокировать множество атак. Но данная настройка требует немалых затрат, а так же необходимо постоянно обновлять ее при изменении или обновлении приложений.

Кроме этого необходимо проводить мониторинг и аудит СУБД. Из-за постоянных изменений в многоуровневой архитектуре корпоративных сетей, необходимо постоянно контролировать пользователей системы в соответствии с их текущими должностями и особенно обращать внимание на привилегированных пользователей. Кроме этого нужно контролировать и пользователей баз данных осуществляя мониторинг и доступа на уровне приложений, и прямого доступа на уровне СУБД. Для предотвращения утечки информации, необходимо чтобы вся активность была прозрачной.

Решения класса DAM позволяют контролировать все сессии СУБД (входы, SQL-код, выходы и т.п.), всех исключений СУБД (ошибки, неудачные попытки авторизации), блокировать нежелательные сессии, оповещать о всех событиях ИБ. Кроме мониторинга активности в БД, решения класса DAM помогают управлять изменениями объектов СУБД и окружения, управлять уязвимостями СУБД. Для предотвращения утечки информации из баз данных производится проверка извлекаемой информации, поиск аномалий в функционировании, автоматическое обнаружение и классификации критичных данных.

Для борьбы с несанкционированным доступом и подозрительными действиями со стороны пользователей используются различные политики безопасности, которые помогают ограничивать доступ к БД или конкретным ее частям по различным параметрам, например учетные записи пользователей, IP-адреса, MAC-адреса, сетевые протоколы, время суток и т.д.

Помимо этого Решения класса DAM предоставляют полный отчет по всей активности системы с возможностью дальнейшего расследования событий информационной безопасности. Таким образом, модно просмотреть работу всех пользователей, обнаружить возможные ошибки и при этом не будет негативного влияния на производительность системы.

Однако необходимо понимать, что все рекомендации по применению средств защиты информации и обеспечения безопасности СУБД подразумевают не только технические средства, но и построение процессов управления информационной безопасностью, составление инструкций и регламентов, а так же распределение ответственности между пользователями информационной системы.

УДК 338.45 : 004.35

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
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

УМЕНЬШЕНИЕ РИСКОВ ИСПОЛЬЗОВАНИЯ «ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ» ПРИ ИСПОЛЬЗОВАНИИ ETOKEN

Использование информационных технологий (ИС), дает огромные преимущества как для отдельных лиц и организаций, так и для общества в целом. Существует множество примеров того, как их использование сделало бизнес более продуктивным и эффективным, позволяя своевременно реагировать на запросы потребителей.

К сожалению, риски при использовании информационных технологий также возрастают и часто приводят к катастрофическим последствиям. Количество «цифровых угроз» безопасности и инцидентов возросло в последние годы, что привело к значительным экономическим и социальным последствиям для государственных и частных организаций, а также физических лиц.

Средства массовой информации ежедневно приводят примеры деструктивного использования возможностей информационных технологий, приводящих к прямым финансовым и репутационным потерям, громким судебным процессам, утрате конкурентоспособности и потери доверия клиентов. Требования информационной безопасности для функционирования ИС стало, по крайней мере, так же важно для современных компаний, как и защита материальных, физических активов. Рост использования Интернета привел к тому, что компании вынуждены сталкиваться с глобальными угрозами.

Информационные системы управления предприятием содержат конфиденциальную информацию, которая должна храниться в безопасности в любой момент времени.

Процесс регистрации пользователя в любой информационной системе состоит из трех взаимосвязанных последовательно выполняемых процедур: идентификации (процедура распознавания субъекта по его идентификатору. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные относятся к нелегальным), аутентификации (процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует) и авторизации (процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации). Профили пользователей необходимо настраивать таким образом, что бы конкретные пользователи имели доступ к конкретным разделам данных, необходимых для их работы, что уменьшит риски утечки информации и неправомерного использования данных.

Каждый пользователь современных компьютерных систем сталкивается с процедурами аутентификации неоднократно в течение рабочего дня. Он вынужден помнить и вводить пароли, ключи и другие идентификаторы. Чем идентификаторы сложней — тем выше уровень защиты, но тем сложнее пользователю их запомнить. Секретные идентификаторы должны быть доступны только пользователям имеющим на это право, так как если злоумышленник может получить закрытый идентификатор какой-либо из сторон, участвующих в информационном обмене, то он легко может расшифровать все сообщения, посланные этой стороне и он может подписать любое сообщение от имени легального пользователя и исполнить его роль в информационном обмене. В таком случае ни о какой информационной безопасности здесь не может быть и речи.

Исследования показывают, что 74% финансовых потерь связано с проблемами так называемого «человеческого фактора». Для сравнения, потери от вирусных и хакерских атак составляют соответственно 4% и 2%.

Данная проблема может найти решение при использовании внешнего аппаратного устройства для хранения идентификатора авторизации в ИС, на основании которого, пользователь, становится легальным. Затем происходит процедура аутентификации, на основании некоторого секретного пароля, известного пользователю. И далее происходит

авторизация пользователя – для каждого пользователя в ИС определяется набор правил, которые он может использовать при обращении к ресурсам системы.

Требования информационной безопасности к экономическим ИС могут быть удовлетворены при применении механизмов «прозрачного» шифрования передаваемой и хранимой информации. Вне зависимости от использованных технологий, легальный пользователь вводит в ИС ключ шифрования, после которого возможна работа с данными. Теперь риск состоит в том, что злоумышленник может иметь доступ к секретному ключу. Проблема состоит в том, что секретный ключ импортируется в небезопасную среду локального компьютера.

Решить эту проблему можно, используя внешнее устройство, подключаемое к персональному компьютеру, способное аппаратно выполнять криптографические операции. Таким образом, внешнее устройство должен быть оснащено микропроцессором, способным зашифровать или расшифровать данные, переданные на это устройство ИС с локального компьютера пользователя. Благодаря такой возможности выполнения криптографических операций, аппаратные устройства обеспечивают более высокий уровень защиты ключевой информации, так как секретные ключи никогда не экспортируются из этого внешнего устройства.

Современные информационные технологии начинают активно использовать возможности технологий «облачных вычислений». Но когда дело доходит до оценки рисков информационной безопасности с одной стороны и функциональностью, удобством использования «облачных» технологий с другой стороны, появляются большие сомнения в возможности переноса бизнеса на «облако».

Современные средства аутентификации и хранения ключевой информации пользователей должны не только обеспечивать защищенное хранение данных в памяти устройства, но и аппаратно поддерживать выполнение криптографических операций в доверенной среде в соответствии с требованиями национальных и международных стандартов.

Использование таких защищенных устройств — eToken, предназначенных для строгой аутентификации и безопасного хранения ключей шифрования, цифровых сертификатов и любой другой секретной информации, обеспечивающих аппаратное исполнение криптографических операций в доверенной среде, позволит значительно снизить риски использования «облачных технологий». Бизнес информация будет храниться на «облаке» в зашифрованном виде и доступ к ней будет иметь только тот пользователь, которому предоставлено на это право. Именно пользователь, владеющий внешним аппаратным устройством, предназначенным для строгой аутентификации и безопасного хранения ключей шифрования, цифровых сертификатов и любой другой секретной информации, обеспечивающем на аппаратном уровне шифрование ресурсов ИС, которое будет поддерживать работу и интегрируется со всеми основными системами и приложениями, будет иметь доступ к ресурсам ИС.

УДК 004.056.01

Бойченко Олег Валерьевич
д.т.н., профессор,
Бояджан Сергей Владимирович
студент 3-го курса бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

АСИММЕТРИЧНАЯ МЕТОДОЛОГИЯ ШИФРОВАНИЯ ДАННЫХ

Асимметричное шифрование - это метод создания ключей, где первый(открытый) ключ является общедоступным и им зашифровывают данные, а другой, секретный, применим для их расшифровки.

Методология данного вида шифрования наиболее актуальна для рассмотрения, т.к. в ней решается одна главная проблема шифрования закрытого типа – найти наиболее безопасный способ передачи ключей.

В данной методологии открытый ключ известен всем, любой из участников шифрования передаёт его по открытым каналам связи другому участнику, однако второй ключ, расшифровки данных, остаётся в секрете.

Данные зашифровываются с помощью открытого ключа, а расшифровать их способен лишь собственник секретного ключа.

Основой для этой методологии послужили так называемые односторонние функции. Они обладают таким свойством: при любом значении неизвестного x не составляет труда посчитать значение функции f(x), однако, если известно значение функции y = f(x), то довольно сложно найти значение x. Например, функция SIN.

Современная криптография стала гораздо более устойчивой к криптоанализу, чем некогда используемые, устаревшие методики, для взлома которых было достаточно ручки и листа бумаги.

Тем не менее, криптоанализ пока ещё рано списывать со счетов.

Во-первых, неизвестно, насколько эффективны применяемые спецслужбами методы криптоанализа, а во-вторых, за годы становления и совершенствования современной компьютерной криптографии было высказано множество претензий как к теоретическим, так и к практическим криптографическим примитивам:

- в 1998 г. было обнаружена уязвимость к атакам на основе шифротекста у блочного шифра MADRYGA, предложенного ещё в 1984 г., но не получившего широкого распространения;
- целая серия атак со стороны научного сообщества, многие из которых были целиком практическими, буквально уничтожила блочный шифр FEAL, предложенный как замена DES в качестве стандартного алгоритма шифрования, но также не получивший широкого распространения;
- также было установлено, что при помощи широко доступных вычислительных средств поточные шифры A5/1, A5/2, блочный шифр CMEA, и стандарт шифрования DECT, используемые для защиты мобильной и беспроводной телефонной связи, могут быть взломаны за считанные часы или минуты, а порою и в режиме реального времени;
- атака методом грубой силы помогла взломать некоторые из прикладных систем защиты, например, CSS— систему защиты цифрового медиаконтента на DVD-носителях.

Таким образом, хотя наиболее надёжные из современных шифров являются гораздо более устойчивыми к криптоанализу, чем Энигма, тем не менее криптоанализ по-прежнему играет важную роль в обширной области защиты информации.

Асимметричные системы часто подвергаются атакам с помощью прямого перебора ключей, и для обеспечения надёжной защиты данных должны использоваться ключи намного длиннее, чем симметричных криптосистемах, для обеспечения идентичной защиты.

На данный момент существует множество различных алгоритмов шифрования с помощью открытого ключа, такие как:

- обмен ключами Диффи — Хелмана;
- алгоритм RSA;
- шифросистема Эль-Гамаля др.

Наиболее популярным является метод шифрования Эль-Гамаля, который разработан на основе одного из вариантов алгоритма Диффи-Хеллмана.

Таким образом, это усовершенствованная система шифрования Диффи-Хеллмана в составе двух алгоритмов, которые использовались для шифрования и для обеспечения аутентификации.

В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию.

Главным недостатком данного метода является довольно низкая скорость работы из-за больших объёмов данных.

Например, 80-бит симметричному ключу соответствует 768-бит асимметричный ключ.

Недостатком схемы шифрования Эль-Гамаля является также удвоение длины зашифрованного текста по сравнению с начальным текстом.

Главным преимуществом схемы цифровой подписи Эль-Гамаля является возможность вырабатывать цифровые подписи для большого числа сообщений с использованием только одного секретного ключа.

Таким образом, чтобы злоумышленнику подделать подпись, ему нужно решить сложные математические задачи с нахождением логарифма в поле Z_n.

Вероятностный характер шифрования также является преимуществом для схемы Эль-Гамаля, так как у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования.

К достоинствам также необходимо отнести то, что при использовании асимметричной системы участники не обязаны встречаться или знать друг друга и иметь секретные каналы связи. Это особенно актуально в случае большого количества участников.

Другим не менее важным преимуществом выступает то, что происходит линейная взаимосвязь числа людей от числа ключей, а не квадратичная как в симметричной системе. Также преимуществом выступает длина ключа.

В асимметричных системах она не имеет значения, поскольку он находится в открытом доступе.

Следовательно, и длина расшифровывания не столь важна.

Данный метод очень удобен для применения не только специалистами, но и обычными людьми во многих назначениях:

- как средство опознавания пользователей и создания цифровых подписей;
- как эффективное средство защиты персональных данных;
- как средство для распределения секретных ключей, которые в последствие будут использоваться в шифровании симметричным методом.

Важным вариантом использования асимметричного шифрования является получение цифровой подписи (электронной подписи), являющейся методом аутентификации отправителя, подтверждающего достоверность сведений об оригинальности содержания переданного документа

УДК 004.056.5

Бойченко Олег Валерьевич,
д.т.н., профессор
Дячук Виктория Сергеевна,
аспирант
Макаренко Андрей Константинович
студент 4-го курса
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

КРИПТОЗАЩИТА КАК ОСНОВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

На сегодняшний день уровень информационный безопасности государства является определяющим фактором его развития и места на мировой арене. Под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Данное определение указано в Доктрине информационной безопасности Российской Федерации, принятой указом Президента РФ № 646 от 5 декабря 2016 года.

В основу информационной безопасности положен уровень безопасности информации, то есть её защищенность, которая состоит в обеспечении конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных. Вышеуказанные критерии можно охарактеризовать как функции обеспечения защиты данных (рис. 1.).

Рис. 1. Функции обеспечения безопасности информации
Источник: составлено автором

Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях является криптография. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить их, сделав бесполезными для незаконных пользователей.

Рассмотрим основные механизмы криптозащиты, такие как шифрование, цифровая подпись и аутентификация. Каждый из механизмов имеет своей целью выполнение определенной функции обеспечения безопасности информации:

1) конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.;

2) целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования;

3) аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Шифр представляет собой совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Здесь зашифровыванием информации называется процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют расшифровыванием (дешифрованием). Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

В основе построения криптостойких систем лежит многократное использование относительно простых преобразований, так называемых криптографических примитивов. Клод Шеннон известный американский математик и электротехник предложил использовать подстановки и перестановки. Схемы, которые реализуют эти преобразования, называются SP-сетями. Ниже приведены основные криптографические примитивы и их использование:

1. Симметричное шифрование. Заключается в том, что обе стороны-участники обмена данными имеют абсолютно одинаковые ключи для шифрования и расшифровки данных. Данный способ осуществляет преобразование, позволяющее предотвратить просмотр информации третьей стороной.

2. Асимметричное шифрование. Предполагает использовать в паре два разных ключа — открытый и секретный. В асимметричном шифровании ключи работают в паре — если данные шифруются открытым ключом, то расшифровать их можно только соответствующим секретным ключом и наоборот — если данные шифруются секретным ключом, то расшифровать их можно только соответствующим открытым ключом. Использовать открытый ключ из одной пары и секретный с другой — невозможно. Каждая пара асимметричных ключей связана математическими зависимостями. Данный способ также нацелен на преобразование информации от просмотра третьей стороной.

3. Хеширование. Преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют, хеш-кодом, контрольной суммой или дайджестом сообщения (англ. message digest). Результаты хэширования статистически уникальны. Последовательность, отличающаяся хотя бы одним байтом, не будет преобразована в то же самое значение.

Таким образом, криптозащита как инструмент обеспечения информационной безопасности является основой для формирования механизмов максимальной защиты данных от их искажения, кражи и незаконного присвоения.

УДК 004.056.05

Бойченко Олег Валерьевич
д.т.н., профессор,
Костенко Н.А.
студент 3-го курса бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

СОВРЕМЕННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛОЩАДОК

Актуальность решения проблем информационной безопасности в управлении деятельностью современного экономического предприятия, ориентированного на сетевые технологии и виртуальную среду, не вызывает сомнений.

Так, согласно исследованиям, общая структура обеспечения информационной безопасности предприятия должна включать следующие подсистемы:

– управления доступом, регистрации и учета;
– антивирусной защиты информации;
– подсистемы межсетевого экранирования;
– подсистема обнаружения вторжений;
– подсистемы анализа защищенности;
– защиты каналов передачи данных (криптографические средства).

Как показывает практический опыт, комплекс технологической документации по обеспечению режима информационной безопасности электронной торговой площадки включает:

– Инструкцию по порядку доступа пользователей в компьютерную сеть;
– Инструкцию о порядке действий в нештатных ситуациях;
– Инструкцию по порядку резервного копирования и архивирования информации;
– Инструкцию по обеспечению работоспособности ЛВС;
– Инструкцию по организации антивирусной защиты;
– Инструкцию по организации парольной защиты;
– Инструкцию по регламентации работы администратора и начальника отдела организации.

Выполнение работниками организации требований данных инструкций позволяет избежать сбоев в обработке информации средствами вычислительной техники.

Данные разрозненные нормативно–правовые акты, регламентирующие обеспечение безопасности информации, объединяются в единый документ верхнего уровня – политику информационной безопасности.

Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на обеспечение информационной

безопасности в информационных системах, включая бумажный документооборот и обмен речевой конфиденциальной информацией.

Политика информационной безопасности представляет пакет документов, включающих головной документ – «Политика информационной безопасности» и документы, регламентирующие процессы обеспечения информационной безопасности, деятельность должностных лиц инфраструктуры информационной безопасности и пользователей информационных систем организации.

Цель политики – выработать и утвердить единые требования и правила, способные обеспечить надлежащую защиту информации и бесперебойную работу информационных систем организации свести к минимуму возможный ущерб от их эксплуатации посредством разработки эффективных превентивных и восстановительных мер противодействия угрозам безопасности.

Документ описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности, а также устанавливает должностных лиц, являющихся ответственными за реализацию политики ИБ и поддержание ее в актуальном состоянии.

В случае использования виртуальной среды для организации экономической деятельности, общая структура обеспечения информационной безопасности предприятия должна включать следующие подсистемы:

– управления доступом, регистрации и учета;
– обеспечения целостности;
– антивирусной защиты информации;
– подсистемы межсетевого экранирования. Программное обеспечение TrustAccess является распределенным межсетевым экраном высокого класса защиты с функцией централизованного управления и аудита событий информационной безопасности и предназначено для защиты рабочих станций и серверов локально–вычислительной сети от несанкционированного доступа, разграничения сетевого доступа к информационным системам предприятия. Внедрение данного программного обеспечения не требует изменения структуры существующей сетевой инфраструктуры. Программное обеспечение может быть использовано как для защиты физических, так и виртуальных машин, как в сетях с доменной структурой, так и в одноранговых. Используя TrustAccess можно разграничить доступ к сетевым службам при взаимодействии в терминальной среде, разделить права доступа к сетевым ресурсам на основе уровней допуска или должностных инструкций сотрудников;
– подсистема обнаружения вторжений;
– подсистемы анализа защищенности;
– защиты каналов передачи данных (криптографические средства).

Обеспечение безопасности в joomla осуществляется путем:

– резервного копирования и восстановления Akeeba Backup Core;
– защиты административной зоны jSecure Lite;
– защиты от спама osolCaptcha;
– защиты от SQL- иньекций RSFirewall;
– проверку на подлинность бесплатного SSL- сертификата от StartSSL.

Стоит заметить, что важным требованием к применяемым средствам защиты является наличие действующих сертификатов ФСТЭК и ФСБ (в части криптографических средств защиты).

С целью повышения эффекта защиты рабочих станций и серверов от несанкционированного доступа возможна также установка электронного замка «Соболь», который является аппаратно-программным средством защиты компьютера от несанкционированного доступа, реализующим функции доверенной загрузки.

Электронной замок «Соболь» реализуется следующие возможности:

– аутентификацию пользователей;
– блокировку загрузки операционной системы со съемных носителей;
– обеспечение контроля целостности программной инфраструктуры;
– обеспечение контроля целостности системного реестра операционной системы;
– обеспечение контроля конфигурации компьютера или сервера;
– функцию сторожевого таймера;
– регистрацию попыток доступа к компьютеру или серверу.

Таким образом, использование современных программно-аппаратных средств защиты обеспечивает условия для надежного управления деятельностью современного экономического предприятия, использующего сетевые технологии.

УДК [005.336.1/. 922.1 : 007] : 51-7

Гапонов Андрей Иванович
к.ф.-м.н., доцент
Смирнова Оксана Юрьевна
ассистент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАСЧЕТ ЭФФЕКТИВНОСТИ КРИТЕРИЕВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время общество переживает информатизацию, проникающую во все сферы человеческой деятельности. В связи с этим процессом появились угрозы для безопасности различных видов информации, использующиеся социумом. Таким образом, особую актуальность приобретает такое явление, как информационная безопасность данных. Сложившаяся ситуация в информационном пространстве требует организацию единого юридического поля для защиты информации в сетях, а также для субъектов, создающих информационные угрозы. Защита информации -база методов и средств, которые обеспечивают конфиденциальность, целостность, доступность, достоверность, аутентичность информации в условиях потенциальной опасности, различного характера.

В Российской Федерации определены: принципы стандартизации Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании"; правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004" Стандартизация в Российской Федерации. Основные положения". Также существует Международный стандарт ИСО/МЭК 15408:2005, разработанный Совместным техническим комитетом ИСО/МЭК СТК 1 "Информационные технологии", Подкомитет ПК 27 "Методы и средства обеспечения безопасности ИТ". ИСО/МЭК 15408 под названием "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий", состоит: Часть 1. Введение и общая модель; Часть 2. Функциональные требования безопасности; Часть 3. Требования доверия к безопасности. ИСО/МЭК 15408 предоставляет возможность для сравнения итогов независимых оценок безопасности, ориентирован на защиту информации от несанкционированного проникновения и трансформации. Существует определенная система информационной безопасности, состоящая из следующих критериев:

- конфиденциальность (confidentiality, C) – доступ информации только условному числу пользователей;
- целостность (integrity, I) – гарантия представления информации в изначальном виде и качестве;
- доступность (availability, A) – возможность получения и обработки информации авторизованным пользователем в необходимый момент.
- дополнительные критерии (additional criteria, AC) **–** управляемость, релевантность, гарантия доставки, важность, аутентичность, апеллируемость.

Расчет комплексной оценки (КО) для критериев информационной безопасности выполним на основе теории нечетких множеств. Уровень критериев, формирующих комплексную оценку, будет определяться в соответствии с оценками 10 экспертов. Причем каждому из этих критериев эксперты дают качественную оценку: *«Н»* – неудовлетворительно, *«У»* – удовлетворительно, *«Х»* – хорошо, *«О»* – отлично. Для окончательного вывода, применяем алгоритм теории нечетких множеств с использованием пакета Fuzzy Logic Toolbox в среде MATLAB. Рассматриваемые критерии соответствуют лингвистическим переменным с такими же названиями. Выходная лингвистическая переменная – «Комплексная оценка» (КО). Эти лингвистические переменные содержат по четыре лингвистических терма с треугольными функциями принадлежности.

$$\mu(x, a, b, c) = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-c}, & a \le x \le b, \\ \dfrac{c-x}{c-b}, & b \le x \le c, \\ 0, & x \ge c, \end{cases} \quad (1)$$

где параметры a и c являются абсциссами концов основания треугольника, b – абсцисса его вершины (см. рис. 1).

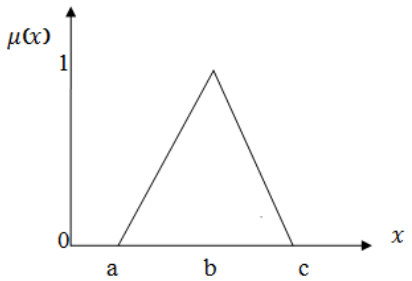


Рисунок 1 - График треугольной функции принадлежности

Параметры функций принадлежности лингвистических термов $\mu_{C;I;A;AC;KO}(H;У;X;O)$ следующие: «*Н» (0; 0; 2), «У» (2; 4; 6), «Х» (6; 8; 10), «О» (10; 12; 12)*. Значения функций принадлежности для входных лингвистических переменных определяем как отношение числа ответов *«Н», «У», «Х», «О»* к общему числу опрошенных. Нечеткий вывод выполняем на основании алгоритма Мамдани. Составляем базу знаний из правил вида: Если С есть «*У*» («*Х*», «*О*»), и I есть «*Н*» («У», «*Х*»), и *А* есть «У» («*Х*», «*О*»), и *АС* есть «У» («*Х*», «*О*»), то *КО* есть «*Н*» («У», «*Х*», «*О*»). Например, если С есть «У», и I есть «Х», и А есть «Х», и АС есть «О», то КО есть «У». Результирующее нечеткое множество для каждого правила (подзаключения) определяем как результат конъюнкции для входящих в него нечетких множеств. Нечеткое множество, соответствующее выходной переменной, является результатом дезъюнкции нечетких множеств, определяемых каждым подзаключением. Каждая комбинация значений входных переменных определяет нечеткое множество, соответствующее выходной переменной. Объединение этих множеств определяем как результирующее нечеткое множество для выходной переменной. Окончательное значение КО находим посредством процедуры дефаззификации для выходной нечеткой переменной по методу «центра тяжести».

УДК 681.5.03

Дячук Виктория Сергеевна,
аспирант
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

АЛГОРИТМ АВТОМАТИЗАЦИИ СНЯТИЯ И ПЕРЕДАЧИ КОММЕРЧЕСКИХ ДАННЫХ ЭЛЕКТРОЭНЕРГИИ

Введение. Информационная безопасность на сегодняшний день занимает ведущее место в формировании информационного общества, способствует устойчивому развитию страны, а также определяет место государства на мировой арене. В Доктрине информационной безопасности, утвержденной Указом Президента от 5 декабря 2016 года, информационная сфера определена как основополагающая сфера в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Также следует отметить, что к национальным интересам в информационной сфере отнесено «обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации … и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время».

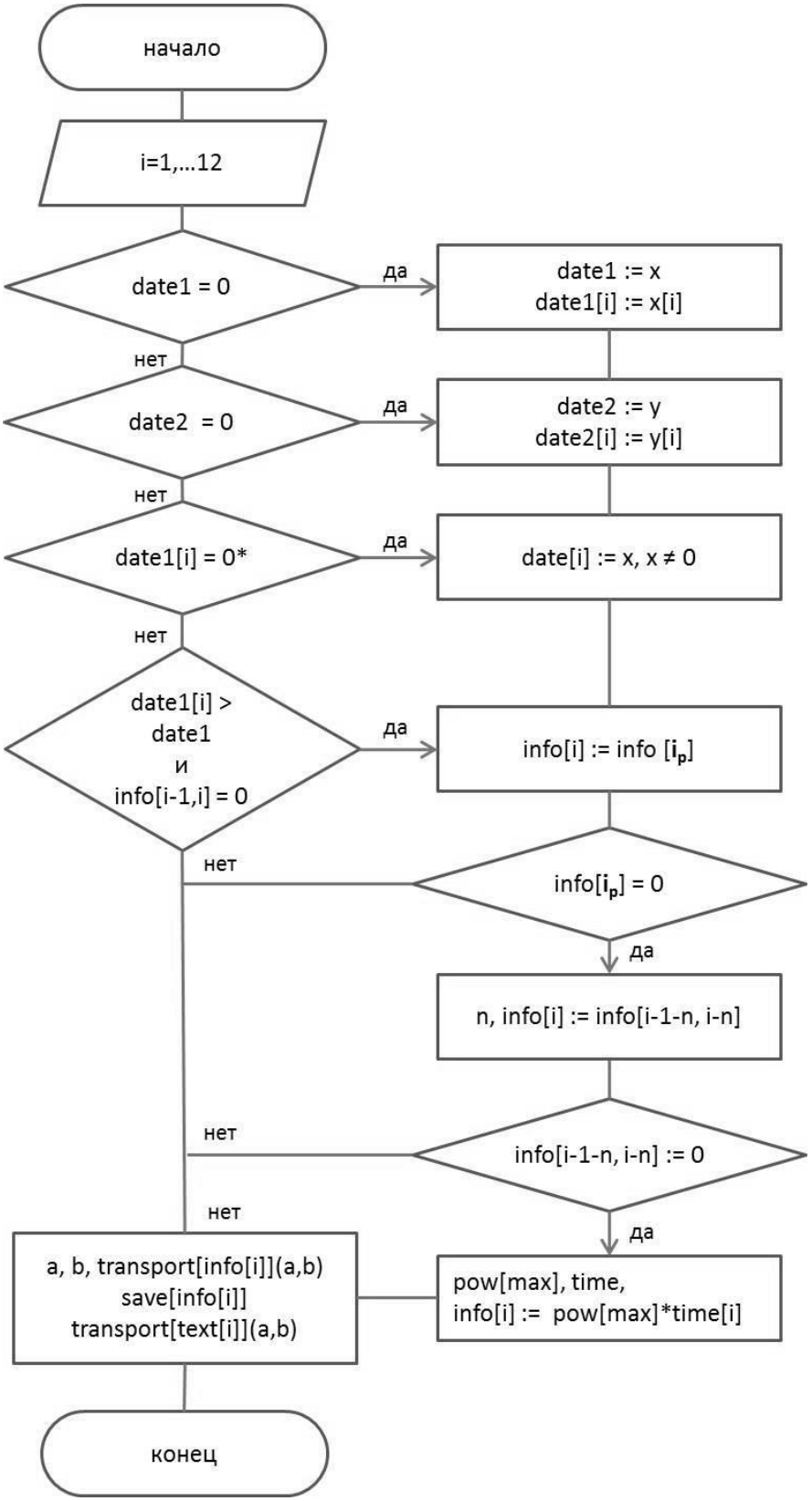


Схема 1. Алгоритм программы автоматизации коммерческого учета данных электрической энергии

Источник: составлено автором

Автоматизация как инструмент информационной безопасности обеспечивает сохранность данных в системе во время совершения операций. По данным исследования The Global State of Information Security Survey 2016 в 2015 году в более чем 35% случаев источниками инцидентов нарушения информационной безопасности являются действующие и бывшие сотрудники компаний. Большинство из нарушений, совершенных пользователями в

системе, являются несанкционированными, что свидетельствует о низкой эффективности защитных механизмов автоматизированных систем. Алгоритм автоматизации системы коммерческого учета электроэнергии, представленный в данной работе, носит характер минимизации влияния человеческого фактора в процессах сбора и передачи информации, так как основывается исключительно на цифровых технических устройствах и технологиях.

За основу построения алгоритма автоматизации положены Требования ГУП «Крымэнерго» к организации коммерческого учета электроэнергии. Согласно данному документу были определены основные переменные, условия и зависимости, представленные далее.

1. День снятия показаний date1 устанавливается либо договором, либо строго равна 00.00 1-го числа месяца, следующего за отчетным;
2. День передачи показаний date2 устанавливается либо договором, либо строго равна 16.00 1-го числа месяца, следующего за отчетным;
3. В случае выходного дня или праздника при снятии показаний date1 (нерабочий день в производственном календаре), дни снятия date1 и передачи показаний date2 переносятся на ближайший предшествующий рабочий день;
4. Акт снятия показаний приборов text передается другой стороне договора в течении 3 рабочих дней с момента снятия показаний date1;
5. В случае непредставления своевременно данных о показаниях прибора в течении 1 -го и 2-х расчетных периодов, объем потребленной электроэнергии устанавливается равным данному периоду предшествующего года;
6. В случае непредставления своевременно данных о показаниях прибора в течении 3 -х и более расчетных периодов, объем потребленной электроэнергии (согласно приложению №3 к ппрф№ 442, далее – постановление) вычисляется как info[i]=pow[max]*time[i].

Алгоритм программы автоматизации коммерческого учета данных электроэнергетики представлен блок-схемой.

УДК 004.942

Зайцева Ирина Владимировна
к.ф.-м.н., доцент
Резеньков Денис Николаевич
к.т.н., доцент
Шлаев Дмитрий Валерьевич
к.т.н.
ФГБОУ ВО «Ставропольский государственный аграрный университет»
Россия

МОДЕЛИРОВАНИЕ НАДЁЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Для информационной системы важным принципом построения является надежность, т. к. информационная система должна быть максимально защищена от несанкционированного доступа к информации, а также полностью отображать информационные и функциональные параметры. Надежность информационной системы обеспечивается с помощью средств адекватных назначению и масштабу системы в процессе хранения и обработки данных. А также следует особо выделить безотказное выполнение функций информационной системой в течение срока эксплуатации.

В общем случае процесс функционирования информационной системы на этапе эксплуатации складывается из чередующихся фаз: транспортировки, хранения, подготовки к работе (транспортировке, хранению), техническому обслуживанию и применению по назначению (работе), наличие и порядок чередования которых зависят от назначения и решаемых ими конкретных задач и условий их применения.

Таким образом, в процессе функционирования информационная система может находиться в одном из некоторого множества состояний (фаз), причем каждое из состояний характеризуется определенным уровнем надежности, т.е. переход из одного состояния в другое определяется показателями надежности информационной системы, в частности «интенсивностями переходов» - условными плотностями вероятностей переходов.

Одним из наиболее распространенных методов исследования состояний информационной системы является метод интенсивностей переходов, основанный на предположении о пуассоновском потоке редких событий, переводящих информационную систему из одного состояния в другое, т.е. поток событий обладает свойствами ординарности и отсутствия последействия.

Для пуассоновского потока:

1) вероятность появления на интервале времени (0,t) m событий равна:

$$P(m, t) = \frac{a^m}{m!} e^{-a} \quad , (m = 0, 1, 2, \ldots),$$

где a – математическое ожидание числа событий на участке от t_0 до $t_0+\tau$, равное $a = \int_{t_0}^{t_0+\tau} \lambda(t)dt$,

$\lambda(t)$ - интенсивность (плотность) потока событий, причем для простейшего потока $\lambda(t) = \lambda =$ const.

2) интервал времени между событиями распределен по экспоненциальному закону.

При таких предположениях, возможно, составить и решить систему дифференциальных уравнений А.Н. Колмогорова. Для этого строится ориентированный граф, вершинами которого являются состояния информационной системы, а направленные ребра - интенсивности и направления возможных переходов.

Рассмотрим на примере исследование состояний информационной системы, которая может находиться в двух состояниях: работоспособном (S_1) и неработоспособном (S_2). Тогда граф состояний рассматриваемой информационной системы имеет вид (рис. 1).

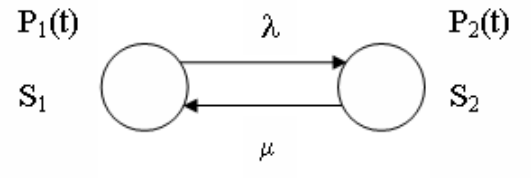


Рисунок 1 - Граф состояний

где λ - интенсивность простейшего потока отказов информационной системы, μ - интенсивность простейшего потока восстановлений работоспособности информационной системы.

Дифференциальные уравнения А.Н. Колмогорова согласно приведенных выше правил примут вид:

$$\left.\begin{aligned} \frac{P_1(t)}{dt} &= -\lambda P_1(t) + \mu P_2(t), \\ \frac{P_2(t)}{dt} &= \lambda P_1(t) - \mu P_2(t) \end{aligned}\right\}$$

Поскольку состояния S_1 и S_2 несовместимы, т.е. составляют полную группу событий, то $P_1(t) + P_2(t) = 1$.

Задавая различные начальные условия (при t = 0), с помощью преобразований Лапласа получим значения вероятностей $P_1(t)$ и $P_2(t)$.

а) Пусть $P_1(0) = 1$ и $P_2(0) = 0$, т.е. начальное состояние информационной системы работоспособно. Используя преобразования Лапласа, получим:

$$\left.\begin{aligned} sF_1(s) - 1 &= -\lambda F_1(s) + \mu F_2(s), \\ sF_2(s) &= \lambda F_1(s) - \mu F_2(s) \end{aligned}\right\}.$$

Переходя от изображений к оригиналам, получим,

$$P_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}, \quad P_2(t) = 1 - P_1(t) = \frac{\mu}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}.$$

б) Пусть $P_1(0) = 0$ и $P_2(0) = 1$, т.е. начальное состояние информационной системы неработоспособно. Тогда аналогично получим:

$$P_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\mu}{\lambda+\mu} e^{-(\lambda+\mu)t}, \quad P_2(t) = 1 - P_1(t).$$

Таким образом, полученные соотношения позволяют определить вероятности двух состояний информационной системы в произвольный момент времени t из различных начальных состояний.

Подводя итог можно сделать вывод, что не существует единственного критерия, достаточно полно характеризующего ясность сложной системы. Это объясняется ее многофункциональностью, надежности сложной системы зависят такие ее показатели, как качество, объективность, долговечность, готовность, безопасность, живучесть и риск. При этом для обеспечения высоких показателей необходимо, чтобы сложная система была высоконадежной и удовлетворяла требованиям по множеству критериев, таких как вероятность безотказной работы, среднее время безотказной работы, наработка на отказ, функция и коэффициент готовности и др

УДК 338 : 004.7.056.53

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОТКРЫТЫХ РАСПРЕДЕЛЕННЫХ МУЛЬТИАГЕНТНЫХ ВИРТУАЛЬНЫХ БИЗНЕС-СРЕДАХ

Вопрос обеспечения информационной безопасности в мультиагентных системах (МАС) может рассматриваться в разных аспектах. Во-первых, необходимо обеспечить защиту от агентов-шпионов и скрытых атак вредоносных программ для узлов сети. Во-вторых, требуется обеспечить защиту от влияния запущенных на узлах сети приложений на самих агентов. В-третьих, следует обеспечить защиту от атак агентов-шпионов, мигрирующих между узлами сети для агентов МАС. Первой поставленной проблемой является защита от атак агентов-шпионов узлов МАС, что решается методами жесткой аутентификации исполняемого программного кода агентов, контроля целостности кода программ-агентов и ограничения прав доступа непосредственно к самим программам-агентам, либо к информации или услугам, предоставляемыми ими. Второй проблемой является информационная безопасность агентов – одна из главных нерешенных задач на сегодняшний день. Это объясняется существованием большого количества вредоносных программ, которые могут несанкционированным путем манипулировать конфиденциальной информацией, которой оперируют агенты и воздействовать непосредственно на процесс функционирования агентов. Решением третьей проблемы может быть создание специальных протоколов безопасности обмена сообщениями между агентами в мультиагентной среде.

Среди основных угроз информационной безопасности распределенных МАС можно выделить: несанкционированный доступ к данным, несанкционированный пассивный перехват сообщений в процессе межагентных коммуникаций, нарушение целостности данных, передаваемых по сети, перехват запросов с дальнейшим их воспроизведением и модификацией, отказ в обслуживании (DDoS-атаки), отказ от факта отправления или получения информации и т.д. Мультиагентная среда уязвима для любой из перечисленных угроз, т.к. ей характерны децентрализованный тип построения, с отсутствующим единым центром, гетерогенность компонентов, потенциальная возможность сообщения с любым узлом.

Из наиболее эффективных и гибких методов решения задач обеспечения информационной безопасности агентов и МАС на сегодняшний день можно выделить: 1) методы мобильной криптографии; 2) метод защищенных состояний агентов; 3) методы организации систем доверительных самоорганизующихся отношений; 4) модель безопасности Бадди (Buddy Security Model); 5) модель безопасности Ксюдонга (POM Security Model); 6) методы, базирующиеся на применении алгоритмов конфиденциальной связи и прокси-сервера, который выполняет функции ограничения и разграничения доступа к ресурсам и сервисам на основе методов идентификации и аутентификации. Однако ни один из приведенных подходов не обеспечивает полного, комплексного решения проблем информационной безопасности от воздействия вредоносных узлов и программ-шпионов для агентов в открытых МАС.

Рассматривая МАС в среде Интернет-бизнеса, можно отметить, что виртуальная бизнес-среда имеет мультиагентную реализацию с точки зрения общей логики функционирования. Выраженность агентной ориентированности проявляется в том, что в ней каждый фактический субъект инновационной деятельности имеет представителя в виде одного или нескольких мобильных программных агентов, которые позиционируют бизнес-предложения своих владельцев и реализуют процедуры автоматизированного поиска бизнес-партнеров для сотрудничества.

Решение задачи обеспечения информационной безопасности в открытой мультиагентной виртуальной бизнес-среде (ОМАВБС) может быть достигнуто двумя основными способами. Первый метод основан на идее закрытой сети «Closed Network» и состоит в создании в ОМАВБС независимых друг от друга агентных платформ (виртуальных площадок) используя технологии, благодаря которым функционируют агенты с похожими целями и интересами (группирование агентов по интересам в закрытые «частные» группы), а также применение метода защищенных состояний агентов для избежания скрытых атак вредоносных программ и агентов-шпионов. Создание виртуальных бизнес-площадок (ВБП) основывается на методе поддержки распределенного реестра одноранговых узлов с неявной древовидной организацией и осуществляется путем выражения целей агентов в виде древовидных концептуальных моделей предметной области. ВБП может быть представлена или выделенным узлом в сети, или группой узлов, создающих закрытую частную подсеть, или часть адресного пространства агентного представительства (частная группа агентов по интересам), воплощенного на одном из узлов системы.

Второй подход подразумевает создание в ОМАВБС специального программного элемента – системы безопасности мобильных агентов (СБМА), отвечающей за реализацию криптографических методов и алгоритмов защиты агентов системы от разных компьютерных атак со стороны вредоносных программ, а также использующей средства имитационного моделирования в целях исследования, прогнозирования и анализа динамики поведения агентов системы. Средствами моделирования могут являться комплексы агентных или системно-динамических моделей. В целях увеличения возможностей функционала СБМА в ее состав интегрированы специально разработанные программные компоненты, которые обеспечивают поддержку самоорганизации агентов и межагентного взаимодействия и реализующие механизмы защиты агентов системы от разных компьютерных атак со стороны вредоносных программ. К таким компонентам относятся: 1) сервер открытых ключей шифрования, который содержит набор индивидуальных открытых ключей для шифрования данных, которыми оперируют агенты системы при взаимодействии друг с другом и с приложениями, запущенными на узлах сети; 2) реестр серверов, который хранит данные о функционирующих узлах системы, а также ведет контроль появления новых агентов и подключения новых узлов в системе; 3) модуль шифрования данных, который реализует процедуры аутентификации и идентификации агентов и криптографические методы защиты данных с открытым ключом; 4) система управления агентами; 5) сервер имен агентов, который собирает данные об агентах системы; 6) специальный реестр «доска объявлений»;

Следует отметить, что ОМАВБС, реализованная с системой децентрализованного управления безопасностью (максимально возможный отказ от централизованных общесистемных сервисов обеспечения безопасности), имеет более высокую надежность и устойчивость к внутренним и внешним угрозам информационной безопасности в целом, а также дает возможность создать эффективную защиту узлов и агентов системы от прямого воздействия агентов-шпионов и вредоносных программ. Среди преимуществ такого подхода реализации СБМА можно выделить адаптируемость, гибкость и распределение нагрузки по обеспечению информационной безопасности между серверными узлами системы и управляющими агентами, несмотря на весьма большую загруженность каналов коммуникации и большое количество информации в обороте.

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Карпова Анастасия Александровна
студентка
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ БРОНИРОВАНИЯ

Ежедневно каждый человек, имеющий компьютер или любую другую вычислительную технику, использует множество автоматизированных информационных систем. Такие системы используются, как для повышения качества частной жизни человека, так и для оптимизации бизнес - процессов предприятия. С появлением сети Интернет автоматизированные системы всё больше популяризируются, их интерфейс упрощается и становится доступным для широких масс населения.

Одной из систем, упрощающих жизнь человека, и одновременно помогающих фирмам получать большую прибыль, является компьютерная система бронирования (КСБ). Данные системы содержат массивные базы данных, соединяют различные организации между собой и позволяют в реальном времени обмениваться информацией и выполнять функции бронирования. КСБ появились в 60-х годах прошлого века в США и СССР. Изначально системы использовались для бронирования билетов на регулярные рейсы авиакомпаний, однако теперь их широко применяют на любые туристические услуги, подлежащие бронированию, например, аренда автомобиля, номера в отеле, экскурсии.

Большую долю пользователей компьютерных систем бронирования составляют туроператоры. Для подключения к общей сети туроператора необходимо установить специализированные программные средства. Интерфейс таких программ чаще всего напоминает командную строку, и работа с ней требует специальных навыков. К сожалению, сегодня в отечественных ВУЗах, предоставляющих образование в области туристического бизнеса, студенты не получают практических навыков работы с компьютерными системами бронирования, к тому же, программные средства, разработанные зарубежными фирмами не всегда адаптированы для российского рынка.

Для удобства клиентов на основе КСБ разрабатываются и функционируют Web-порталы с доступным интерфейсом. А использование глобальной сети порождает новые проблемы информационной безопасности: хищение или несанкционированный доступ представляют опасность для коммерческой составляющей предприятия, а компьютерные вирусы и атаки хакеров несут угрозу технической стороне. Владельцы таких порталов обязаны должным образом обеспечивать информационную безопасность не только для своего предприятия, но и для клиента, ведь зачастую при бронировании клиент использует личную информацию (паспортные данные, реквизиты банковских карт и прочее). Следовательно, при обмене информацией с клиентом необходимо использовать защищенные каналы связи и/или шифрование информации.

В соответствии с законодательством организации, предоставляющие услуги бронирования, при передаче персональных данных обязаны использовать сертифицированные шифровальные средства и иметь лицензию на работу с ними. По факту такую лицензию имеют немногие. Решением этой проблемы может стать формирование органов контроля. Следовательно, проблемы информационной безопасности туристического бизнеса должны решаться на уровне целой отрасли или даже в масштабах государств.

УДК 338

Круликовский Анатолий Петрович
к.ф.-м.н.,доцент
Кравцов Игорь Олегович
студент
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

РОЛЬ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В настоящее время задача обеспечения информационной безопасности предприятия почти полностью лежит на руководителе организации. А основой для принятия тех или иных решений является информация. Поэтому получение искаженной информации или несанкционированный доступ к последней может нести большую угрозу безопасности предприятия.

Вся деятельность организации базируется на информационных системах, и стороннее вмешательство в одну из них, например, в электронный документооборот, приведет к негативным последствиям. Противодействует таким угрозам комплекс мероприятий, обеспечивающий целостность, конфиденциальность и доступность информации – все это по сути является обобщенным определением понятия информационная безопасность.

Обеспечение информационной безопасности – трудоёмкий и ресурсоёмкий процесс, требующий внимательности, так как цена ошибки может быть очень велика. Программные средства, помогающие в работе над такими задачами, называют системами поддержки принятия решений (СППР). Применение экспертных СППР для обеспечения информационной безопасности организации очень эффективно, так как, во-первых, экспертные системы поддержки принятия решений рассчитаны на использование большим числом специалистов и аккумуляцию большого объема знаний экспертов высшей категории, во-вторых, благодаря применению специально разработанных математических алгоритмов появляется возможность решения неструктурированных задач. Обеспечение информационной безопасности состоит из нескольких этапов, таких как определение ценности информации, выделение угроз, уязвимых мест в деятельности организации, выбор средств управления рисками, формирование задачи оптимизации обеспечения информационной безопасности, принятие решения о мерах безопасности, непосредственное их внедрение и контроль. СППР решают оптимизационную задачу и генерируют варианты мероприятий по обеспечению информационной безопасности. Для этого в СППР необходимо внести информацию о стоимости ресурсов организации, вероятности рисков, потерях в случае их наступления и затратах на средства защиты. При заданных значениях рисков система определяет оптимальный набор мер защиты, затраты на которые не превышают потерь от реализации угроз.

В данный момент существуют СППР, использующие когнитивные технологии. Такие современные интеллектуальные системы поддержки принятия решений как IBM Watson, при обеспечение доступа как к массивам внутренней информации, так и к глобальной сети, способны обучиться и самостоятельно выделять риски и вероятности их наступления для предприятия, а также предлагать меры для их минимизации или устранения. Ещё одной важной функцией интеллектуальных СППР является помощь при распределении полномочий и доступа к информации.

Несмотря на то, что СППР вполне способны помочь руководителю сделать правильный выбор или обезопасить информационные системы предприятия от нежелательного вмешательства, последнее решение всегда должно приниматься уполномоченным лицом.

УДК: 519.852.3

Матвеев Владимир Васильевич
к.ф.-м.н., доцент
Титаренко Виктор Николаевич
старший преподаватель
Титаренко Дмитрий Викторович
к.э.н., доцент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

МОДЕЛЬ ЗАДАЧИ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ПРОИЗВОДСТВЕННОЙ РАСПРЕДЕЛИТЕЛЬНОЙ СИСТЕМЫ

Постановка задачи. Пусть производственная система потребляет некоторый ресурс (вода, газ, нефтепродукты). Структура системы имеет вид:

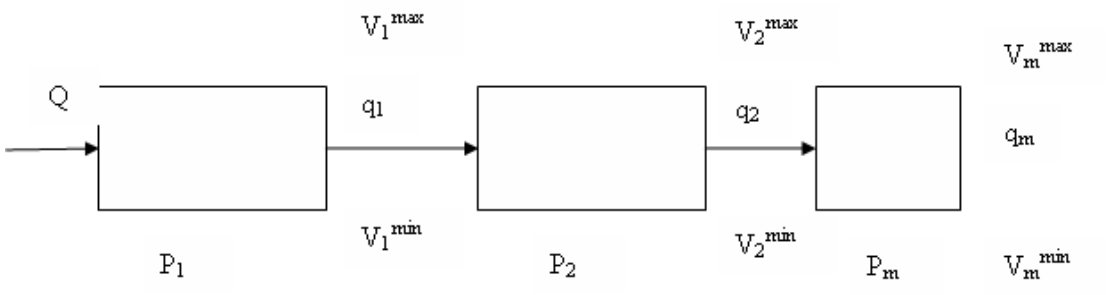


Рис. 1. Схема производственной распределительной системы

$P_1, P_2, ..., P_m$ - производства, потребляющие ресурс,

τ_i - время транспортировки ресурса между (i-1) и i-м объектами,

$q_1(\tau), q_2(\tau), ..., q_m(\tau)$- потребление ресурса соответствующим потребителем в момент времени τ,

$V_1^{min}, V_1^{max}, V_2^{min}, V_2^{max}, ..., V_m^{min}, V_m^{max}$ - минимальные и максимальные емкости резервуаров ресурса m-го потребителя.

Емкости резервуаров необходимы для компенсации неравномерного потребления ресурса m-ым потребителем.

Игровая постановка задачи. Пусть игрок P сообщает свое управление в виде вектора заказов $(q_1(t), q_2(t), ..., q_m(t))$ известно на период времени $t = \sum_{i=1}^{N} \tau_i$. Ограничения запасов заданы вектором:

$$V_i^{\min} \le V_i\left(t + \tau_i^m\right) \le V_i^{\max},\ i = 1, ..., m$$

Вектор управлений игрока Р (потребителей):

$$\overline{q_m}(\tau) = \left\{ q_i\left(\tau + \theta_i^m\right), i = \max\{1, m-1\}, ..., N \right\}$$

Вектор управлений игрока Е (поставщика ресурса):

$$\overline{Q_m}(t) = \left\{ Q_i\left(\tau + \theta_{i-1}\right), i = \max\{1, m-1\}, ..., N \right\}$$

С течением времени заказы меняются, т.е. в момент времени τ информация о векторе $\overline{q_m}(\tau)$ может меняться.

При выборе в момент времени τ вектора $\overline{Q_m}(\tau)$ используется только информация вектора $\overline{q_m}(\tau)$, а информация о значении $\overline{q_m}(\theta),\ \theta > \tau$, считается неизвестной.

Задача управления системой может быть сведена к дифференциальной игре удержания запасов, динамика которой описывается уравнением (1).

$$V_{N-1}^{\min} - V_{N-1}(0) \le \alpha_{N-1} \int_{-\tau_{N-1}}^{0} Q_{N-1}(\tau)dt - \int_{0}^{\tau_{N-1}} Q_N(\tau)dt - \int_{0}^{\tau_{N-1}} q_{N-1}(\tau)dt \le V_{N-1}^{\max} - V_{N-1}(0)$$

$$V_N^{\min} - V_N(\tau) \le \alpha_N \int_{0}^{\tau_{N-1}} Q_N(\tau)dt - \int_{0}^{\tau_{N-1}} q_N(\tau)dt \le V_N^{\max} - V_{N-1}(\tau) \quad (1)$$

Для нормального функционирования системы необходимо удерживать объемы ресурса в заданных пределах, т.е. выполнять систему неравенств (1).

Терминальное множество задается неравенством (2):

$$V_i^{\min} \le V_i\left(t + \theta_i^m\right) \le V_i^{\max},\ i = \max\{1, m-1\}, \ldots, N \quad (2)$$

$\overline{Q_m}$, $\overline{q_m}$ - управления игроков Е и Р соответственно. Стратегия игрока Р, гарантирующая окончание игры в его пользу может быть выбрана не единственным способом.

Задачу обеспечения удержания объемов рассмотрим в качестве ограничений, и выбор управлений Q_m осуществляется согласно двух критериев.

Критерий 1. Минимизация числа переключений управления $Q_m(\tau)$.

В рамках первого критерия вводится второй критерий

Критерий 2. Связан с определением надежности функционирования системы.

Согласование критериев. Если в какой-либо момент времени τ управление игрока Е можно не переключать, то значение вектора управлений остается прежним. Если τ - момент переключения, то выбор вектора $Q_m(\tau)$ подчинен второму критерию.

Функционал выигрыша игрока Р связана с вероятностью выполнения неравенств (1)

УДК 510

Ремесник Елена Сергеевна
ассистент
Институт экономики и управления
ФГАОУ ВО «КФУ им.В.И. Вернадского»
Республика Крым, Россия

МАТЕМАТИКА В КРИПТОГРАФИИ

Криптография прочно вошла в нашу жизнь. Когда мы разговариваем по телефону GSM или LTE шифруют наш голос и SMS-сообщения, чтобы их нельзя было перехватить. Когда заходим на сайт по протоколу HTTPS, то все данные также шифруются с помощью криптографии. При пользовании банковских карт тоже неявно используем криптографию. Проследим развитие криптографии и рассмотрим, какие науки являются основой современной криптографии.

Как наука криптография сформировалась не более ста лет назад. Однако первые шифры появились более трех тысяч лет назад (скитала, шифр Цезаря). Первоначально шифры и криптография развивались достаточно медленно: с момента использования и придумывания шифра Цезаря и до первых реальных попыток взломать его прошло несколько столетий. Если заметить, самые активные стадии развития криптографии связаны с военными действиями. Во время различных войн странам понадобилось активно защищать свою информацию. К началу первой мировой войны появились государственные конторы, которые занимались криптоанализом на высоком уровне (Россия, Франция, Великобритания). Во время второй мировой войны активно использовалась одна из первых электромеханических машин «Энигма». И уже после второй мировой войны получила развитие математическая криптография.

Зарождение математической криптографии относят примерно к 60-70 г.г. XX века. Это время появления активных разработок в области теории чисел, общей алгебры и других математических областях, которые позволили построить шифры, используемые и сейчас. Важным этапом в развитии математической криптографии стала стандартизация симметричного шифра под названием DES. Сейчас этот алгоритм устарел и ему на смену пришел новый

алгоритм AES. Данные алгоритмы относятся к классу симметричных алгоритмов, позволяют быстро шифровать большое количество данных, но возникает сложность при обмене ключами. Рассмотрим некоторые алгоритмы, относящиеся к асимметричной криптографии. Алгоритм Диффи-Хеллмана, используемый для получения секретного ключа, был предложен в 1976 году. Если рассматривать с математической точки зрения, то данный алгоритм работает с натуральными числами, используется понятие простых чисел и принципы деления с остатком. Его стойкость основана на сложности дискретного логарифмирования, поэтому перебор всех комбинаций пока остается сложной вычислительной задачей даже для современных компьютеров. Однако этот алгоритм все же уязвим — подвержен атаке типа «man-in-the-middle». Алгоритм RSA кроме шифрования данных позволяет применять электронные цифровые подписи. Используемые основные математические понятия: простые числа, взаимно простые числа, деление с остатком, возведение в степень по модулю (данная операция заложена в основу шифрования, так как относится к односторонним функциям), малая теорема Ферма, китайская теорема об остатках, расширенный алгоритм Евклида. Стойкость алгоритма основана на задаче факторизации, являющейся в настоящее время вычислительно сложной. Каждый класс алгоритмов имеет свои достоинства и недостатки. Симметричное шифрование происходит быстрее, но сложнее распределять ключи и сохранить их секретность при обмене. Асимметричное шифрование более трудоемко, однако легче произвести обмен ключом. Оптимальный вариант шифрования (по скорости и сохранению секретности) — это использование комбинации данных алгоритмов. С помощью алгоритма RSA создается общий ключ, а далее с помощью симметричного алгоритма происходит шифрование самого сообщения. Строгое математическое обоснование стойкости имеет только симметричный алгоритм, поэтому в военных и правительственных организациях ему отдается предпочтение.

Криптография — это наука, объединяющая в себе такие науки как математика и информатика. Используются последние разработки в теории функций, теории вычислимости, общей алгебры и других математических областей. Таким образом, развитие в области криптографии напрямую зависит от развития математических наук и, конечно, последних разработок информационных технологий. Новые математические открытия, связанные с преодолением сложности вычислений, заставят полностью пересмотреть современную криптографию.

УДК 004.58

Семенова Юлия Андреевна
старший преподаватель
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИССЛЕДОВАНИЕ УГРОЗ ДЛЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ ОБЛАКА И МЕТОДЫ ЕЕ ЗАЩИТЫ

В настоящее время дата-центры следующего поколения размывают границы между физическими и виртуальными средами, между публичными и частными облаками, что приводит к расширению ряда вопросов по защите информации в облачных вычислениях. Обеспечение физической безопасности базируется на основе строгого контроля физического доступа к серверам и сетевой инфраструктуре. Сетевая безопасность основана на построении надежной модели угроз, учитывает защиту от вторжений и межсетевой экран, с целью разграничения внутренних сетей дата-центров на подсети с различным уровнем доверия.

В облачных вычислениях технология виртуализации играет особую роль и заключается в:

- виртуализации серверов – перенос физических серверов в виртуальные машины одной хостовой системы, оснащенной гипервизором – средством виртуализации;
- виртуализации рабочих пользовательских мест – централизованное хранение доступа по сети с физических рабочих мест;
- виртуализации терминалов – для отдельного пользователя терминала в операционной системе создается собственный сеанс работы.

Концепция облачных технологий заключается в предоставлении пользователям удаленного динамического доступа к услугам, вычислительным ресурсам и приложениям, включая операционные системы и инфраструктуру через различные каналы доступа, в том числе и через Интернет. Такая крупномасштабная инфраструктура представляет повышенные риски и

весьма ограниченную возможность контроля над ее ресурсами. В этом и заключается актуальность проблем облачных вычислений – защита информации и доверительное отношение пользователей к облачным провайдерам.

Применение специализированного программного обеспечения для виртуальной среды требует значительного изменения в подходах к обеспечению информационной безопасности облачных систем. Решение задач обеспечения безопасности объединяет в себе традиционные и специфические решения с особенностями, которые в процессе выполнения задач должны оптимизироваться для экономии производительности виртуальной среды с обеспечением защиты информации и облачных ресурсов.

Для обеспечения безопасности и сохранения целостности данных исследуются актуальные угрозы для виртуальной инфраструктуры «облака»:

- отсутствие контроля внутрисетевого трафика, а также возможность прослушивания всего трафика между виртуальными машинами;
- единое хранилище виртуальных машин, над которыми можно получить несанкционированный контроль;
- захват всех ресурсов хоста виртуализации одной виртуальной машиной, в результате которого другие виртуальные машины могут вызвать отказ в обслуживании;
- незащищенность уязвимых мест дисковой подсистемы виртуальных машин;
- компрометация клиентских терминалов и атака на браузеры клиентов;
- несанкционированный доступ к ресурсам виртуализации через гипервизор из виртуальной или реальной среды;
- перехват аутентификационных данных для доступа к «облаку» через облачные API;
- несанкционированный доступ к консоли управления виртуальной средой;
- отсутствие в виртуальной инфраструктуре распределенных коммутаторов, которые при миграции виртуальных машин позволяют согласовывать политику безопасности;
- перехват данных при передаче по незащищенным внешним каналам связи.

Одним из главных источников угрозы безопасности является сервер централизованного управления виртуальной инфраструктуры, получив контроль над которым, злоумышленник получает полный доступ ко всем виртуальным машинам, хостам виртуализации, виртуальных сетей и хранилищ данных. Поэтому необходимо, в первую очередь, тщательно защищать сам сервер управления, обращать усиленное внимание на средства аутентификации и разграничения прав доступа, для чего имеет смысл использовать дополнительное программное обеспечение, разработанное специально для виртуальных инфраструктур. Доступ к серверу виртуализации должен осуществляться безопасными протоколами, а доступ администраторов должен быть ограничен по IP-адресам.

Важно также, чтобы сети управления виртуальной инфраструктурой и производственной средой виртуальных машин были разделены логически и физически для предотвращения несанкционированного вмешательства.

Для обеспечения защиты данных в «облаке», расположенных за пределами сферы физического доступа клиента, осуществляют шифрование виртуальных жестких дисков. При считывании с диска данные расшифровываются и при записи на диск зашифровываются. При этом ключи хранятся на отдельном сервере управления ключами, который сначала проверяет идентификационные данные и целостность облачного сервера, который направил запрос. В случае положительного отзыва предоставляется ключ, и облачный сервер получает доступ к информации.

Более мощный вариант безопасности данных представляет собой комбинирование технологий шифрования данных и защищенной передачи.

Для повышения безопасного использования облачных технологий целесообразно использовать системы обнаружения вторжений и межсетевого экранирования с контролем внешних подключений к среде виртуализации с помощью аппаратных решений, а внутренних - с помощью программных решений, реализуя, таким образом, комбинированный подход.

Быстро выявить атаки злоумышленника позволяют журнальные записи, сделанные серверами «облака», которые служат важным источником информации при проведении инженерно-технических экспертиз. Поэтому сохранение журнальных записей за весь срок службы облачного сервера является важной, необходимой мерой и позволит осуществить дальнейший анализ сбора данных, их объединения и вывода на внешние инструменты, платформу безопасности или на систему управления событиями информационной безопасности.

Следующими эффективными средствами защиты «облаков» являются:

- доверенные загрузки серверов виртуализации, виртуальной машины, серверов управления виртуализацией;
- сегментирование виртуальной инфраструктуры для обработки персональных данных пользователем или группой пользователей;
- идентификация и аутентификация доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

Для антивирусной защиты виртуальных машин лучше использовать безагентный подход, обеспечивающий комплексную безопасность без установки агентского модуля в защищаемой системе, то есть в виртуальную среду внедряется виртуальное устройство – шлюз безопасности, который берет на себя функции антивируса для всех виртуальных машин.

Верно подобранные решения безопасности позволяют получить представление об уровне используемых ресурсов и своевременно выявить атаки, которые нацелены на различные облачные объекты.

Для снижения операционных расходов, связанных со средствами защиты систем виртуализации, рекомендуется использовать специально разработанное программное обеспечение, адаптированное для облачных вычислений.

Но все же еще остаются проблемы адаптации защиты виртуализации в «облаке», которые требуют дальнейшего анализа и усовершенствованного решен

Солдатов Максим Александрович
доцент, к.ф.-м.н.
Солдатова Светлана Александровна
старший преподаватель
Адарчина Светлана Олеговна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ ЗАДАЧ РАСПОЗНАВАНИЯ ЛИЦ НА ПРИМЕРЕ FACE-ТРЕКЕР

Актуальность исследования заключается в необходимости защиты данных, используемых в инновационном продукте, в процессе создания которого применялась технология нейронных сетей и машинного обучения.

Качественная нейронная сеть – это, прежде всего, качественное обучение нейронов. Обучение заключается в настраивании весов между нейронными связями при решении задач по оптимизации методом градиентного спуска. Во время обучения нейронной сети автоматически извлекаются характерные черты, определяется их важность, и происходит построение связей между ними. В конечном результате нейронная сеть может воспользоваться опытом, полученным в ходе обучения на незнакомые образы за счет объединения способностей.

Среди всего разнообразия видов нейронных сетей в области распознавания лиц стоит выделить сверточную. Именно сверточная нейронная сеть позволяет учитывать двумерную топологию изображения в отличие от многослойного перцептрона. Характеризуется такая сеть следующими признаками:

1) локальные рецепторные поля (наличие локальной двумерной связи нейронов);

2) общие веса (детектирование частей изображения и уменьшение числа весовых коэффициентов);

3) иерархическая структура с пространственными подвыборками.

За счет вышеперечисленных особенностей сверточная нейронная сеть обеспечивает относительную устойчивость к небольшим изменениям изображения, в частности: масштаба, положения, поворота, освещения, смены ракурса и т.д. Экспериментальные исследования сверточной нейронной сети на базе данных ORL показали 96% точность распознавания изображения лица с изменениями эмоций, поворотами головы и т.д.

Свое развитие сверточная нейронная сеть получила в инновационной разработке Face-трекер – сценария, который позволяет автоматически распознавать клиентов, новых и тех, кто пришел повторно. Все данные о визитах – будут сохраняться в карточке клиента в CRM, где в последствии можно будет отследить историю взаимодействия с клиентом. На основании такой информации можно делать клиенту персонализированный подход, увеличивая вероятность продажи.

Однако, на сегодняшний день остро стоит вопрос о необходимости обеспечения информационной безопасности. Безопасность персональных данных обеспечивается и регулируется федеральным законом №152 «О персональных данных». Информация о клиентах, партнерах, конкурентах превратилась в самый дорогой товар, так как информация в руках мошенника — это орудие преступления, в руках уволенного сотрудника — средство мести, в руках инсайдера — товар для продажи конкуренту. Именно поэтому персональные данные Face-трекера нуждаются в самой серьезной защите

УДК 519.688: 519.872

Солдатов Максим Александрович
к.ф.-м.н., доцент,
Солдатова Светлана Александровна
старший преподаватель
Тупота Елена Сергеевна
студентка бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАЗРАБОТКА СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ НА БАЗЕ ПРОГРАММНОГО СРЕДСТВА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ANYLOGIC

Введение. При ведении любой коммерческой деятельности на данном этапе развития современного общества важнейшим аспектом является использования средств имитационного моделирования. Построение грамотной имитационной модели может помочь предпринимателю сгенерировать конкретную ситуацию и оценить возможности предприятия для полного грамотного функционирования.

Постановка проблемы. Моделирование представляет собой совокупность методов решения особого класса задач. Смысл такого подхода заключается в замене реальной системы более упрощенной за счет абстрагирования и стандартизации. Моделирование применяется в случае, когда проведение реального эксперимента над существующей системой невозможно по ряду причин (дороговизне, длительности проведения эксперимента, фактору риска и т.д.).

Процесс имитации может пригодиться в любой деятельности, однако нами была принято решения провести данный процесс для бензоколонки.

Целью данного исследования является изучение проблематики аспектов при создании и проверки системы массового обслуживания и ее разработка на базе средств для имитационного моделирования AnyLogic.

Методы исследования. Применение имитационных моделей дает множество преимуществ по сравнению с выполнением экспериментов над реальной системой и других групп методов. Применение имитации при планировании коммерческой деятельности, является ключевым аспектом в деятельности предприятия.

Для решения поставленной задачи необходимо создать многоканальную систему массового обслуживания с ожиданием в очереди и отказом. Система массового обслуживания является системой, которая производит обслуживание клиентов определенными приборами, в нашем случае бензоколонками. В системе такого типа так же необходима очередь, она может быть с накоплением и без. С учетом нашей задачи нам необходимо построить систему с накоплением конечной емкости, так как зачастую некоторые клиенты уезжают не дождавшись своей очереди. Длина очереди не может превышать емкость накопителя, при этом требование, поступающее в переполненную СМО теряется.

Нами была решена задача для бензоколонки с тремя пунктами выдачи товара и очередью с накоплением, возможную длину оператор настраивает сам, благодаря этому разработанная модель может применятся не только на одном предприятии и не только в одинаковых условиях. Результат построения данной модели представлен на рисунке 1.

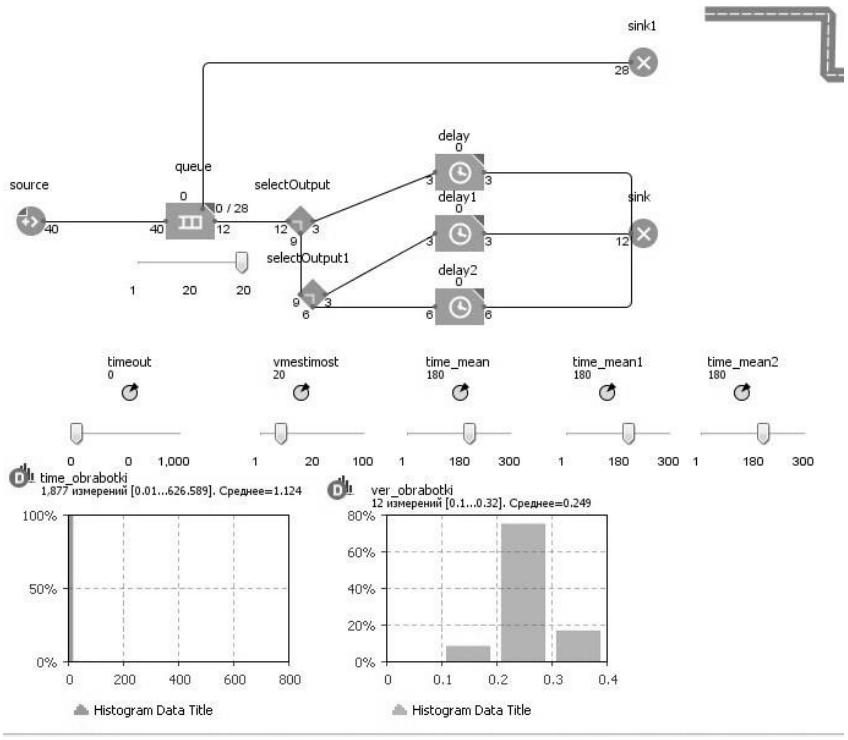


Рис. 1. Имитационная модель Системы Массового Обслуживания Бензоколонки

Так же, нами были добавлены «ползунки», с помощью которых оператор может изменять среднюю длину ожидания в очереди, вместимость очереди, обработку заказа на каждой колонке. Так же, в конце эксперимента, система построит графики, на которых будет отображаться среднее время обработки заказа и вероятность обработки поступающего заказа.

Результаты исследования. Как результат, нами была разработана система массового обслуживания с кастомизацией процесса для бензоколонки с тремя пунктами выдачи. Так же, разработанная модель дает статистику для оператора, что крайне важно для проведения эксперимента.

Выводы. Таким образом, в ходе исследования нами была разработана имитационная модель деятельности бензоколонки, которая может быть внедрена на любом предприятии со схожими параметрами.

УДК 004.58

Акинина Людмила Николаевна
старший преподаватель
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ ЗАЩИТА В ИНТЕРНЕТ-МЕССЕНДЖЕРЕ TELEGRAM

Telegram является бесплатным кроссплатформенный мессенджеров для девайсов, позволяющий обмениваться информацией и медиа файлами различных форматов.

Как и в большинстве мессенджеров, аккаунты пользователей привязываются к мобильному номеру, что является одним из существенных аргументов критиков Telegram, потому что сложно при этом соблюдать полную анонимность. При регистрации на сервисе и при следующих авторизациях новых девайсов, происходит проверка телефонного номера с помощью SMS с кодом (на некоторых ОС — перехватывается приложением) или телефонный вызов.

Количество активных пользователей сервиса на декабрь 2016 г. составляло свыше 100 млн. человек, а количество ежедневно отправляемых сообщений перешагнуло ступеньку в 10 млрд. на январь 2017.

«Телеграм» изначально экспериментально запускался компанией Digital Fortress для проведения теста MTProto на сильных нагрузках.

Новое приложение получило особую версию для Apple iPad, модифицировав техническую поддержку видеороликов и фото высокого разрешения, обеспечило возможность пересылки изображений с анимациями в формате gif. Основатель WhatsApp – Ян Кум – заявил, что его идеи реализованы в Telegram.

Серверы Telegram не хранят информации из засекреченных чатов, однако сохраняют историю обычных чатов и содержимое адресной книги пользователей на период использования клиента и еще по крайней мере на полгода после неиспользования аккаунта. Использованное в мессенджере шифрование не обеспечивает PFS во всех случаях.

Клиент Telegram по умолчанию отправляет рассылку пользователям метаинформацию о открытии или закрытии приложения, при этом подписаться на данную метаинформацию может любой пользователь. С целью отключения такой рассылки необходимо поменять опции аккаунта.

Существуют мнения, что мессенджером могут воспользоваться различные террористические группы как для обмена информацией, так и для пропаганды своих идей. В частности, террористическая группировка ИГ (ИГИЛ) применяла Телеграм с целью распространения личных убеждений более чем 14 тысячам подписчиков в свыше чем 30 потоках на различных языках.

Для мессенджера был создан протокол MTProto, предусматривающий применение нескольких протоколов кодирования. При авторизации и аутентификации применяются алгоритмы RSA-2048, DH-2048 для кодирования, при передаче сообщений протокола в сеть они шифруются AES ключом, известным клиенту и серверу. Кроме того, используются криптографические хеш-алгоритмы SHA-1 и MD5.

Защита от перехвата сообщений сервером обеспечивается только в режиме «засекреченных» чатов (Secret Chats) с 08.10.2013 г., путем кодирования, при котором только отправитель и получатель пользуются единым ключом (end-to-end кодирование).

В отличие от обыкновенного режима, сообщения в секретных чатах не расшифровываются сервером, история переписки сберегается всего на 2-ух устройствах, на которых был сформирован чат.

При обмене файлами возможно, как отправить файлы с самого устройства, так и искать медиа контент в сети интернет для iOS либо Android. Объем транслируемых файлов ограничен до 1,5 Гб. Программа применяет систему докачки файлов, в случае если соединение было оборвано, обеспечивает возможность создавать мультичаты до 200, с ноября 2015г. - до 1000, с 14.03.2016 – до 5000 участников. Все перечисленные достоинства обеспечивают популярность Telegram, который в свою очередь гарантирует достаточно высоких уровень информационной защиты данных в своей среде.

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

ИНФОРМАЦИОННЫЕ ТРЕНДЫ ПОВЕДЕНИЯ ПОТРЕБИТЕЛЕЙ

Информационная безопасность касается не только вопросов защиты информации, но и скорости ее обработки, новых средств получения данных из сети Интернет, рассылки сообщений пользователям о своем бизнесе и реакции на эти рассылки. Поэтому определение причин неудач в Интернет маркетинге связано с новыми тенденциями поведения потребителей, захвате их внимания и соответственно, в трансформации из потенциального покупателя в реального. Актуальность данной темы связана с тем, что, информация меняется быстрыми темпами и возникает проблема не отставать от передовых технологий и избежать провала в бизнесе.

Технологии меняются. Целевая аудитория меняется. Маркетинг меняется. Поэтому развивается тот, кто успевает использовать восходящие тренды.

В ходе исследования были изучены статистические данные, на основании которых можно выделить следующие факты, характеризующие современное поведение целевой аудитории в сети Интернет.

1. Необходимость создания мобильной версии сайта. Так как больше половины аудитории использует мобильные устройства наряду с компьютерами, а пятая часть и вовсе выходит в Интернет только с них. Средний взрослый пользователь проводит 5,6 часов в день в Интернет (по данным Distill Networks, 2015). В среднем человек смотрит в телефон от 180 до 50 раз в день. Поэтому обязательно сайт должен быть адаптирован под мобильную версию.

Рис. 1. Как выходят в сеть пользователи Интернета [Источник: https://yandex.ru/company/researches]

2. Продолжительность концентрации внимания сократилась на 30%: с 12 до 8 сек (по данным Attention Spans: Consumer Insight, Microsoft, 2015). Если оффер (рекламное предложение) не цепляет в течение 8 секунд — оно не зацепит уже никогда.
3. Количество пользователей, блокирующих стандартную рекламу, за год выросло на 124%, с 54 млн до 121 млн (по данным Ad Blocking Goes Mainstream, PageFair. 2015).
   Классические каналы рекламы на Западе уже перестают работать.
4. 40% молодежи проводят больше времени в мессенджерах, чем в социальных сетях (по данным Attention Spans: Consumer Insight, Microsoft, 2015).
5. 59 % трафика генерируют чат-боты (По данным Distill Networks, 2015).
6. 65% пользователей не устанавливают новые приложения (по данным Attention Spans: Consumer Insight, Microsoft, 2015), потому что предпочитают чаты, в чатах больше информации, чат интерактивнее и позволяет создавать обратную связь.
7. 50 % клиентов заключает сделки с тем поставщиком, кто первым ответил на их запрос.
8. Персонализированный подход к клиенту увеличивают конверсию на 14%.

Проблема в том, что становится сложнее привлечь внимание новых клиентов к компании привычными способами. Люди постепенно переходят от компьютеров к мессенджерам и от веб-сайтов к чат-ботам. Стоимость привлечения клиентов тоже растёт. Ещё год-два назад, чтобы получать заявки, достаточно было сделать простой сайт и настроить директ. Сегодня в отдельных нишах аукцион «разогрет» настолько, что стоимость привлечения нового клиента превышает стоимость совершаемой покупки. Поэтому те, кто успевает воспользоваться

восходящими трендами, какими совсем недавно были директ и эдвордс, остаются впереди конкурентов.

Таким образом, то, насколько быстро вы трансформируетесь сегодня — определит, будет ли существовать ваш бизнес завтра. Из всего вышесказанного следует один вывод: скорость важнее денег.

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

СОЦИАЛЬНЫЕ СЕТИ И ЛИЧНАЯ БЕЗОПАСНОСТЬ

Социальные сети, получившие широкое распространение во всем мире и побудившие большое число людей к выкладыванию подробных сведений о своей жизни, несут угрозу не только морального или финансового характера, но и ментального, разрушая сложившиеся миропонимание и создавая ложные представления о фундаментальных процессах и мотивируя асоциальное поведение.

Проблему личной безопасности в социальных сетях рассматривают пока немногие исследователи, среди которых следует отметить О.И. Горобец, С.М. Ненашева, Г.У. Солдатову и О.И. Олькину, Г.З. Ефимову и Е.В. Зюбан. Данная проблема имеет два аспекта: представление индивида в пространстве общества, его внешние официальные и неофициальные данные и внутренне состояние ментального пространства, мысли и чувства, структура долговременной памяти. Соответственно различают информационно-технологическую и информационно-психологическую безопасность пользователей социальных сетей.

К внешнему представлению пользователя Интернет в социальной сети относят данные его аккаунта: сообщаемые сведения о своей биографии, месте проживания, образовании, интересах, выкладываемые фотографии с различных мероприятий. Пользователи могут быть реальными и анонимными, которые выдают себя за совершенно других людей с целью вступления в группы по интересам, знакомству с новыми людьми и, зачастую, с мошенническими намерениями. Если пользователь реальный, но не сообщает о себе достаточно сведений, по которому его можно определить, его связи могут сообщить о нем достаточно сведений, чтобы узнать, где он живет, работает, учился и т.п. В связи с этим, как отмечает С.М. Ненашев, возникают следующие конфликты: между необходимостью открывать личные данные для удобства пользования социальными сетями и желанием пользователя скрыть эти данные; между желанием донести некоторую информацию до своих знакомых и невозможностью затем управлять доступом к этой информации; конфликт интересов физических и юридических лиц, являющихся пользователями социальных сетей. Последний конфликт возникает часто среди журналистов СМИ и редакциями, которые они представляют, т.к. высказанное частное мнение в переписке сети или в блоге журналиста воспринимается как позиция издания, которое он представляет. Это же относится к политическим и общественным деятелям, ведущим собственные блоги. Юридические лица используют социальные сети для проверки кандидатов на рабочие вакансии, рекламу своих товаров и услуг, сбор мнений о их качестве и ожиданиям потребителей. Также физические и юридические лица используют социальные сети для распространения своего информационного воздействия, распускания ложных слухов и компромата. Отследить анонимную публикацию бывает практически невозможно, но многие пользователи сети заводят большое количество неизвестных «друзей», которые создают условия для быстрого распространения непроверенной информации.

Прямыми угрозами для пользователя являются: кража личных данных, фотографий, переписки; использование профиля в мошеннических целях; дискредитация владельца профиля и раскрытие его настоящего имени, если он этого сам не сделал. Примерами мошенничества являются рассылка писем настоящим друзьям с просьбой оказать материальную помощь или заплатить за официальные услуги сети, например, оплатить «ОКи» в «Одноклассниках с последующей кражей этих денег, перевод на свои счета денег с банковской карточки, если ее номер был введен в сети для оплаты официально предоставляемых услуг. Такой вид мошенничества называется фишингом. Прямой угрозой авторитету пользователя, его репутации и, возможно, здоровью, служит троллинг – запугивание и издевательство над пользователем,

организация провокаций со стороны других пользователей. Имеются примеры, когда страдали невинные люди, являющиеся однофамильцами реальных преступников или асоциальных личностей.

Информационно-психологические угрозы безопасности пользователя социальных сетей имеют причины и следствия и относятся к угрозам внутреннего характера для личности. В число причин входит желание самораскрыться, чему способствует онлайн общение. Выкладывая подробную личную информацию, многочисленные фотография из разных мест пребывания, пользователь повышает вероятность использования своей информации другими агентами сети, которые, находя с ее помощью уязвимые в психике места, могут вовлечь индивида в различные группы и организации, ведущие антиобщественную, в том числе, террористическую, деятельность. В социальных сетях практически не существует механизмов защиты личной информации, об этом должен заботиться сам пользователь.

Выделяют три группы пользователей социальных сетей: активные, много пишущие в своих аккаунтах; пассивные, читающие чужой контент и трансляторы – сами не создающие, но активно распространяющие сведения, полученные из сети. Чтение представленного в сети контента оказывает влияние на когнитивные структуры личности – модели знаний (репрезентации) в ее мозге. Замечено, что человек больше прислушивается к мнению своего окружения, пусть и виртуального, чем к официальным источникам, считая преподавателей. Поэтому мнения «друзей», предложения вступить в некоторую группу по «расширению» сознания, ментальным непроверенным практикам, эзотериков и других может навредить мировоззрению молодого или не очень уверенного в себе человека. Такое воздействие еще слабо изучено в силу закрытой информации, подобные группы ограждают себя от внешнего влияния. Особенно нуждаются в ментальной защите дети и подростки, открытые для восприятия любой поступающей информации и не способные ее критически осмыслить. В настоящее время каждый второй ребенок в России пострадал в результате угроз, связанной с персональной информацией в социальных сетях. В связи с этим необходимо учить соблюдать конфиденциальность, критичность восприятия поступающей информации, проявлять осторожность при вступлении в различные группы в социальных сетях.

УДК 330

Соколова Жанна Владимировна
к.и.н., доцент
Таврическая академия
Бакуменко Мария Александровна,
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

МОНИТОРИНГ РЕПУТАЦИИ ПРЕДПРИЯТИЯ КАК НЕОБХОДИМЫЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Репутация предприятия является важнейшим нематериальным активом предприятия и фактором, влияющим на его конкурентоспособность. Ухудшение репутации предприятия – одна из существенных угроз для его успешного функционирования и процветания. Поэтому в настоящее время компании вынуждены постоянно оценивать свою репутацию, иными словами, проводить мониторинг репутации.

На малых предприятиях эти задачи, как правило, входят в должностные обязанности маркетолога или специалиста по связям с общественностью, а в крупных компаниях этими вопросами занимаются целые отделы.

Репутацию предприятия необходимо отслеживать как из офф-лайн, так и он-лайн источников информации. Сформированное мнение о предприятии в Интернет-пространстве имеет даже большую значимость, ввиду всё возрастающей роли Интернет в жизни каждого человека.

Потребители товаров и услуг перед принятием решения о покупке, как правило, знакомятся в Интернет с отзывами о компании, ее продуктах, услугах, сервисе и т. д. Данные отзывы могут быть как реальными, так и «чёрным пиаром» со стороны конкурентов. Существуют тематические он-лайн площадки для написания отзывов. К примеру, в мировом (в том числе отечественном) отельном и ресторанном бизнесе одной из самых широко известных площадок является TRIP ADVISOR - сайт, на котором миллионы путешественников делятся

своими впечатлениями об объектах размещения, питания и развлечений. Недаром один из самых востребованных сервисов бронирования отелей в мире BOOKING.COM также ввёл функционал оставления отзывов.

Информация о компании может быть представлена в Интернет в самых различных формах – в виде отзыва, комментария на форуме, поста или комментария в социальных сетях, в виде новости, интервью, PR-статьи и т. д. Вручную отследить и оценить репутацию компании в он-лайн пространстве очень сложно и практически нереально. Поэтому востребованными являются специальные сервисы в Интернет по мониторингу репутации. Примером такого сервиса является зарубежный сервис Review.Pro. Данный сервис позволяет компании следить не только за изменением своей репутации в Интернет, но и за репутацией конкурентов.

Необходимо отметить, что репутация компании зависит от её реальных действий и не может полностью контролироваться компанией. Поэтому топ-менеджмент компании должен проводить социально ответственную политику и помнить об этических принципах.

УДК 339.137.27

Бойченко Олег Валерьевич
д.т.н., профессор
Адарчина Светлана Олеговна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

МАРКЕТИНГОВЫЕ ВОЙНЫ В ИНТЕРНЕТЕ

Актуальность исследования заключается в изучении современных стратегий и тактик в области интернет-маркетинга.

Развитие инфраструктуры глобальной сети Интернет и коммерцилизация Интернета привели к изменениям способов ведения бизнеса и появлению электронного рынка.

Интернет стал использоваться как интерактивный канал взаимодействия компаний с бизнес-партнерами и клиентами, что обеспечило ведение интерактивного маркетинга (Интернет-маркетинга) и осуществление прямых онлайновых продаж.

Традиционные бизнес-процессы (продажа, маркетинг, снабжение и т.д.) в сетевой экономике приобретают новые формы.

Таким образом, бурный рост электронного бизнеса и электронной коммерции стали основой для появления Интернет-маркетинга (он-лайн маркетинга).

Инструменты Интернет-маркетинг значительно отличаются от традиционных инструментов маркетинга.

Известно, что к основным преимуществам Интернет-маркетинга по сравнению с офф-лайновыми средствами маркетинга относятся:

- широчайший охват целевой аудитории (глобализация рынка);
- персонализация взаимодействия с клиентами;
- снижение транзакционных издержек.

Основным направлением Интернет-маркетинга является продвижение сайта в поисковых системах.

Именно продвижение сайта в поисковых системах является необходимым условием для достижения эффективного взаимодействия с целевой аудиторией или клиентами, так как поисковые системы и тематические каталоги являются основными каналами, по которым целевые посетители попадают на сайт.

Продвижение сайта в поисковых системах - это комплекс всех маркетинговых мероприятий для продвижения сайта в Интернете, чтобы ресурс стал известен целевой аудитории и был посещаем клиентами:

- раскрутка сайта (наращивание ссылочной базы);
- оптимизацию сайта под поисковые системы;
- реклама в Интернете;
- проведение опросов, поддержка общения с клиентами (организация эффективной обратной связи с клиентами, оперативное изучение их потребностей);
- постоянная поддержка сайта, поисковая оптимизация и мониторинг эффективности его функционирования;
- изменение маркетинговых планов в соответствии с меняющейся ситуацией.

- Однако суть маркетинга сегодня заключается вовсе не в обслуживании покупателей — необходимо перехитрить, обойти, победить своих конкурентов.
- Маркетинг — это война, в которой конкурент является противником, а покупатель — территорией, подлежащей завоеванию.
- Главным средством борьбы является информация, где с одной стороны, компании нужны данные о действиях конкурентов, а с другой, компания дает информацию потребителю.

Однако суть маркетинга сегодня заключается вовсе не в обслуживании покупателей — необходимо перехитрить, обойти, победить своих конкурентов.

Маркетинг — это война, в которой конкурент является противником, а покупатель — территорией, подлежащей завоеванию.

Главным средством борьбы является информация, где с одной стороны, компании нужны данные о действиях конкурентов, а с другой, компания дает информацию потребителю.

Очевидно, что цель войны - захват территории противника, его рынка, и увеличение собственной прибыли за счет роста продаж.

Изучив современные тенденции в области интернет-маркетинга, можно предложить следующую классификацию компаний:

1) Лидеры – это компании, занимающие самую большую рыночную долю. Поэтому главной стратегией оборонительной войны является введение новых продуктов, которые позволят избежать ценовых войн с конкурентами и увеличат долю рынка;

2) Претенденты – это компании, которые активно стремятся догнать лидера и увеличить свою долю рынка.

В наступательной войне можно выделить следующие стратегии, основной целью которых является захват рыночных позиций конкурента:

— фронтальная атака – это прямая атака на конкурента с аналогичными линиями продукта, ценами, продвижением;

— фланговая атака – это атака на рыночные сегменты, где конкурент наиболее слаб или отсутствует вовсе;

— круговая атака заключается в распространении продукта во всех сегментах и каналах дистрибуции;

— обходная атака состоит в продвижении в новые или малозначимые поля (новый продукт, новый географический сегмент, новый вид деятельности);

— партизанские атаки заключаются поиске ниши рынка настолько маленькой, чтобы лидерам неинтересно было ее защищать (распродажи, скидки, подарки, розыгрыши и т.д.). Позволяет резко переманить к себе покупателей, а при первой же опасности фирмы готовы будут покинуть свои позиции;

3) Последователи – это компании, повторяющие действия лидера, идущие проверенным путем клонирования, подделки, имитации.

4) Аутсайдеры – это компании, специализирующиеся на одном узком сегменте рынка, работающие исключительно в своем секторе и не пытающиеся развиваться.

Стратегиями аутсайдера являются:

— специализация на одном типе потребителей;

— продажа в одной местности;

— предложение специализированного сервиса, недоступного другим.

Таким образом, грамотное изучение сайтов конкурентов даст много полезной информации, где можно проследить весь процесс привлечения посетителя и конвертации его в покупателя.

Довольно часто встречаются случаи внедрения готовых идей, но использование чужих решений — это также способ перенять чужие проблемы. Поэтому найдя свою нишу в бизнесе необходимо еще приложить усилия, дабы не стать жертвой конкурентов.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Абдуллаева Джемиле Мухитдин-кызы
магистрант
Таврическая академия
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ЛИЧНАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Трудно представить сегодня человека, у которого не было бы аккаунта хотя бы в одном из социальных сетей, а зачастую человек регистрируется в нескольких: Facebook, ВКонтакте, Twitter, Одноклассники, Google+ и др. Социальные сети позволяют расширить круг знакомств, общаться и обмениваться информацией с людьми из зарубежных стран, осуществлять покупки, строить партнерские отношения. Однако, регистрируясь в социальных сетях появляется мера опасности для жизни пользователя и его знакомых. Рассмотрим с какой целью злоумышленники атакуют социальные сети и предложим методы улучшения безопасности.

Одним из видов атак социальных сетей является DDoS атака, которая может использоваться мошенником с целью шантажа, требуя деньги за прекращение атаки, или вести информационную войну. Такой атаке уже подвергались социальные сети Twitter, Flickr и ВКонтакте.

Следующий вид атак является фишинговая атака, целью которой получение конфиденциальных данных пользователя. Осуществляется как массовая рассылка, где указывается ссылки на сайт с редиректом. Как только пользователь переходит на данный сайт, мошенники пытаются путем психологического воздействия узнать логины и пароли, чтобы использовать их для доступа к банковским картам или другим аккаунтам.

Не так давно компания Check Point Software Technologies Ltd обнаружили атаку, которая встраивает вредоносные ПО в графические файлы и изображения, такая атака получила название ImageGate. Она была обнаружена в Facebook и LinkedIn. Во время этой атаки все файлы на персональном устройстве автоматически шифруются, и получить доступ к ним можно только после выплаты выкупа.

Самоатака XSS или межсайтовый скриптинг заключается в том, что в веб-страницу внедряется вредоносный код, который выполняется при переходе на эту страницу и взаимодействует с сервером мошенника. Такой код позволяет отслеживать определенные действия пользователя на “заряженной” странице, например, авторизация.

Существует и много других атак на социальные сети и цель у них одна – получить данные пользователя для вымогательства или прямого перевода денег, для ведение информационных войн. По мере того как хакеры придумывают способы взлома аккаунта, другие программисты улучшают меры безопасности.

Для защиты аккаунта необходимо использовать надежный пароль и логин. Можно также настроить двухфакторную верификацию для доступа. Она предусматривает два этапа входа: ввод логина и пароля, а также уникального кода, отправленного по SMS. Такую настройку поддерживают Google+, ВКонтакте, Facebook, Twitter, LinkedIn.

Протокол HTTPS используется для безопасного соединения. Он обеспечивает шифрование передаваемых данных. В Twitter, Google+, ВКонтакте, Facebook уже используется данное шифрование. На других социальных сетях его необходимо сконфигурировать.

На письма, полученные от имени социальных сетей, необходимо отвечать с сайта-отправителя, чтобы избежать переадресацию на сервер мошенника.

Некоторые социальные сети могут предложить установку программ, созданные сторонними разработчиками. Мало проверяемые программы не следует инициализировать на ПК, поскольку они больше подвержены атаке.

Социальные сети мощный инструмент для обмена информацией и следует применять все меры для защиты личной информации.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Сейтшаев Руслан Рустемович
магистрант
Таврическая академия
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ

Для систем, рассчитанных на постоянную работу, безопасность играет весьма значительную роль. Веб-серверы — это основа Интернета. Они отвечают за базовые услуги и функционирование миллиардов веб-сайтов по всему миру, в результате превращаясь в хранилище персональных данных посетителей. Обеспечение защиты серверов от атаки извне — это одна из важнейших задач любой полагающейся на них организации.

Веб-серверы особенно уязвимы в силу своей открытости — по своей природе они рассчитаны на обмен информацией с пользователями. Злоумышленник может внести модификации в код HTTP сервера или сервера базы данных, или самих страниц веб-сайта, поменяв его изначальную функциональность.

Идеального метода защиты, способного полностью защитить веб-сайт от любого рода внешних атак, на данный момент не существует. Для обеспечения максимальной защиты веб-сервера требуются совместные действия администраторов веб-сайтов, программистов и проектировщиков; такие вещи, как антивирусное ПО, операционные системы и права доступа, требуют постоянного внимания. Ниже будут рассмотрены некоторые методы противодействия компрометации веб-серверов.

Следует вовремя обновлять все программное обеспечение, работающее на веб-сервере. Любое ПО, не относящееся к необходимым компонентам (например, DNS-сервер, либо средства удаленного администрирования, либо службы удаленных рабочих столов), следует отключить или удалить. Если средства удаленного администрирования все же необходимы, нужно следить за тем, чтобы не использовались легко угадываемые пароли.

Правильно настроенный веб-сервер также способствует предотвращению атаки. Одним из наиболее распространенных серверных скриптовых языков является PHP. MySQL — это одна из наиболее популярных СУБД, используемых в сочетании с PHP; она эффективна, достаточно функциональна, а также с простой настройкой и использованием. Прежде всего необходимо корректно настроить файл конфигурации «php.ini».

При установке MySQL создается база данных «test», используемая по умолчанию, и открытая учетная запись «root» без пароля. Данной учетной записи автоматически предоставляется полный доступ ко всем прочим базам данных на сервере. В связи с этим необходимо:

- изменить пароль учетной записи «root»;
- создать новую учетную запись MySQL и предоставить ей необходимые права;
- удалить базу данных «test» и соответствующих пользователей.

Ниже приведены основные правила написания безопасного кода.

- Глобальные переменные всегда следует отключать, поскольку их можно намеренно инициализировать с помощью подложного запроса GET или POST.
- Сообщения об ошибках следует отключить; вместо них следует использовать запись сведений об ошибках в лог-файл.
- Не следует считать надежными данные, поступающие от пользователей; для удаления специальных символов SQL и escape-последовательностей необходимо использовать функции фильтрации.

Обеспечение безопасности веб-сайтов является актуальной темой в наше время. Следуя вышеизложенным рекомендациям, можно существенно снизить риск проведения успешной атаки на веб-сервер. Это позволит избежать заражения посетителей сайта, падения трафика с поисковых систем и возможных проблем с индексацией

УДК 004.056 : 334.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Алейник Денис Павлович
студент
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В последние несколько лет в сфере информационных технологий появилась и начала активно развиваться новая концепция – «облачные вычисления». Этот термин относительно новый как в России, так и во всём мире. «Облачные вычисления» – информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами.

Можно выделить основные преимущества данной технологии:

- Снижение капитальных расходов потребителей на оборудование (расходы поглощаются провайдером облачных услуг).
- Оптимальное использование персонала. Благодаря данной технологии можно рациональней распределять ценных сотрудников, концентрируясь на прибыли, а не на поддержке программного обеспечения.
- Защищенность и идентификация – гибкое управление доступом к физическим и виртуальным машинам, информации и приложениям в центре обработки данных. Благодаря использованию такой платформы идентификации пользователей реализуется защищенный доступ к IT-ресурсам с самых разнообразных устройств.

Перед тем, как рассмотреть основные угрозы и проблемы безопасности, следует определить, какие существуют облачные инфраструктуры, или же «облака».

1. Частное «облако» – предназначено для использования одной компанией, а также её клиентами и подрядчиками.
2. Публичное «облако» – может использоваться широкой публикой. Может находиться в собственности и управлении организаций.
3. Общественное «облако» – вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи.
4. Гибридное «облако» – комбинация из двух или более вышеперечисленных инфраструктур, остающихся при этом уникальными объектами.

Не смотря на то, что «облачные вычисления» могут предложить малому бизнесу значительную экономическую выгоду, необходимо учитывать, что доступ к сложному программному обеспечению сопровождается определенными рисками в области информационной безопасности. ИТ-провайдеры осведомлены о рисках присущим «облачным вычислениям» и стараются предотвратить их.

При выборе потенциальных поставщиков облачных услуг, необходимо учитывать семь основных проблем в области информационной безопасности:

1. Безопасная передача данных. Весь трафик, перемещающийся между Вашей сетью и любым сервисом, к которому Вы получаете доступ в «облаке» ведется через Интернет. Убедитесь, что ваши данные всегда передаются по безопасному каналу, подключайтесь к провайдеру только через URL, который начинается с «HTTPS». Кроме того, ваши данные всегда должны быть зашифрованы и проходить проверку подлинности с использованием стандартных отраслевых протоколов, таких как IPsec (Internet Protocol Security), которые были разработаны специально для защиты интернет-трафика.
2. Безопасные программные интерфейсы. Альянс Облачной Безопасности (The Cloud Security Alliance, CSA) предлагает ознакомиться с программными интерфейсами или API, которые используются для взаимодействия с «облачными» сервисами. CSA рекомендует изучить, как любой поставщик «облачной» инфраструктуры, которого Вы рассматриваете, интегрирует безопасность в его сервис: от методов аутентификации и управления доступом до контрольной политики действия.

3. Безопасность хранения данных. Данные хранимые на сервере провайдера должны быть надежно зашифрованы. Поставщиков «облачной» инфраструктуры, должен обеспечить надежную защиту данных не только во время их передачи, но также и когда они находятся на их серверах. Необходимо знать, насколько надежно провайдеры избавляются от Ваших данных в случае необходимости.
4. Контроль доступа пользователей. К данным, хранившимся на сервере поставщика «облачной» инфраструктуры, может потенциально получить доступ сотрудник той компании, которая пользуется услугами этого поставщика. Провайдер должен предоставить информацию о тех людях, которые управляют Вашими данными, и об уровне доступа, который они имеют к нему.
5. Разделение данных. Каждый сервис «облачных вычислений» делится ресурсами, а именно, местом на серверах провайдера и других частях его инфраструктуры. К примеру, программное обеспечение Hypervisor используется, чтобы создать виртуальные контейнеры на аппаратных средствах провайдера для каждого из его клиентов. CSA отмечает, что «Атаки появились в последние годы, и нацелены на совместно используемые технологии в среде «облачных вычислений». Исходя из этого заявления следует, что необходимо изучить методы управления правами доступа (процесс ограничения прав доступа к информации для тех лиц, которым она необходима для работы), а также применять шифрование данных, хранимых вашим провайдером, для предотвращения доступа в Ваш виртуальный контейнер другими клиентами.
6. Проблемы доступности. Никакая служба не может гарантировать 100%-е время работы. На это влияют множество факторов, например, электропитание, отсутствие соединения с серверами.
7. Юридические риски. Большинство инструкций безопасности данных предназначены, чтобы защитить определенный тип данных. Мало того, что компании защищены этими инструкциями, они также обычно обязаны знать:
    1) Где данные находятся.
    2) Кому разрешен доступ к ним.
    3) Как это защищено.

Если компания заказывает обработку или хранение данных, которые требуют защиты, то поддержание их в защищенном состоянии возлагается на провайдера облачного сервиса. Если у компании нет соответствующей правовой защиты, то в случае утечки данных в «облачном» сервисе, который представляет данные компании, она может быть призвана к ответственности.

Необходимо обсудить эти вопросы безопасности с поставщиком «облачной» инфраструктуры, прежде чем доверить свои данные его серверам и приложениям. Брешь в безопасности Ваших данных или данных Вашего клиента может быть разрушительна в зависимости от типа данных и степени угрозы. Финансовые затрат на исследование и решения проблем, связанных с юридическими расходами, и снижением репутации компании могут быть настолько значительными, что выгодно предпринять усилия по уменьшению рисков информационной безопасности. Риски, связанные с доступностью «облачного» сервиса, менее серьезны, но всё еще несут значительные риски.

Также, отсутствие доступа или контроля может повлечь за собой серьезные проблемы, которые могут обойтись компании в значительную денежную сумму

УДК 338

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Чернова Анастасия Игоревна
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

АУТСОРСИНГ В ЭЛЕКТРОННОЙ КОММЕРЦИИ: ОСОБЕННОСТИ ПЕРЕХОДА И ПРОБЛЕМА БЕЗОПАСНОСТИ

В электронной коммерции модели аутсорсинга применяются чаще, чем в традиционном бизнесе. Это обусловлено прежде всего спецификой бизнеса: любая электронная торговая площадка нуждается в специализированной инфраструктуре, использующей различные технологические и программные решения.

Что же представляет собой аутсорсинг? Аутсорсинг – это делегирование некоторых задач, производственных функций или бизнес-процессов одной компании на обслуживание другой, являющейся профессионалом в рассматриваемой сфере деятельности. Однако, следует понимать, что на аутсорсинг обычно передаются задачи с бесперебойной поддержкой работоспособности отдельных систем компании. Основой служит заключение контракта на определенный период. При этом, чтобы снизить вероятность возникновения возможных рисков, контракт на начальном этапе сотрудничества должен быть краткосрочным и предусматривать осуществление постоянного контроля аутсорсеров.

Различают такие модели аутсорсинга:

- полный (аутсорсеру передается полный комплект функций);
- частичный (передаются отдельные бизнес-процессы);
- управляемый (при передаче аусорсеру определенных задач, остается возможность контроля и распределения работ).

Использование в электронной коммерции моделей аутсорсинга бизнес-процессов и сервисов позволит сократить возможные риски, а также повысит эффективность работы участников.

Выделим основные причины обращения к модели аутсорсинга в электронной коммерции:

1. Избавление от рутинных операций, сокращение штата сотрудников;
2. Оптимизация ИТ-инфраструктуры и сервисов (в основном виртуализация);
3. Интеллектуальная обработка данных (использование уникальных технологий);
4. Развитая инфраструктура аутсорсера (в основном логистическая).

Из-за высокой динамики инновационных процессов, возникает потребность в передаче на аутсорсинг сложных интеллектуальных функций и процессов, эффективность которых в основном зависит от знаний ноу-хау.

Одним из наиболее популярных видов аутсорсинга, применяемых в электронной среде, является Информационно-технологический (ИТ). Свое распространение этот вид аутсорсинга получил за счет технологии облачных вычислений. Cloud Computing предоставляет пользователю компьютерные мощности и ресурсы в виде отдельного интернет-сервиса.

В e-commerce возникает востребованность к логистическому аутсорсингу, что обусловлено инфраструктурными и производственно-технологическими преимуществами поставщиков услуг. Так, в электронной коммерции используют такую форму логистического аутсорсинга, как фулфилмент (fulfllment) – комплексное выполнение процессов продажи, начиная с оформления заказа и заканчивая доставкой до покупателя.

Владельцам электронного бизнеса необходимо постоянно проводить мониторинг актуальных тенденций, из них выбирать наиболее интересные и перспективные, внедрять в свои проекты новые технологии.

Таким образом, преимущества Информационного-технологического аутсорсинга для электронной коммерции следующие:

- возможность самообслуживания по требованию;
- сетевой доступ к ресурсам (для различных платформ через стандартные механизмы);
- создание групп ресурсов (позволит перераспределить инфраструктурные возможности и уменьшить стоимость услуг);
- измеримость результатов обслуживания (проведение автоматизированного мониторинга, использование инструментов для оптимизации);
- эластичность сервиса.

Однако следует понимать, что при передаче на аутсорсинг важных задач, есть риск утечки данных, потери полного или частичного контроля над собственными ресурсами, а также возможно появление конкурента, использующего знания и опыт компании. Сохранение информационной безопасности в аутсорсинге возможно при выполнении таких основных требований:

1. Формирование технологической инфраструктуры, с целью минимизации технологических рисков.
2. Разработка мер по управлению рисками, направленных на минимизацию возможных последствий.

В качестве аутсорсера должна выступать надежная и проверенная временем компания, с опытными и грамотными сотрудниками, исключающая свое банкротство или неожиданный распад.

Подводя итог, отметим, что так как большинство интернет-магазинов используют в работе многофункциональные платформы, осуществляющие анализ и контроль, мониторинг, планирование, то лучшим вариантом можно считать интеграцию этих процессов с функционалом автоматизированных систем аутсорсеров. При этом необходимо постоянно изучать существующие практики ведения бизнеса в Интернет-среде, инновационные предложения, заниматься разработкой новых методик повышения качества и снижения затрат на предприятии.

Мулюкбаева Виктория Юрьевна
студентка
Королев Олег Леонидович
доцент, к.э.н.
Институт экономики и управления
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ФИШИНГ В СЕТИ ИНТЕРНЕТ

Фишинг – это вид мошенничества, при котором преступники создают поддельный сайт, похожий на оригинальный, с целью завладения данными пользователя (чаще всего это логин, пароль от сайта), а также данными по банковским картам. Согласно третьему отчету Microsoft по индексу компьютерной безопасности, опубликованном в феврале 2014 года, ежегодные потери от фишинга по всему миру достигли 5 миллиардов долларов.

Фишинг чаще всего осуществляется с помощью электронной почты. Сообщения приходят пользователю как бы от социальных сетей, банков, платежных систем. В тексте сообщений вставляют ссылки на сайты, которые были созданы мошенниками. Графически эти сайты выглядят так же, как и оригинальные или почти как оригинальные, отличается только адрес сайта, может быть на одну букву.

Виды фишинга

Фишинг-копье – это вид фишинга, который направлен против конкретных лиц или организаций. В этом случае злоумышленники собирают информацию о жертвах, чтобы увеличить шансы на успех. Этот метод является самым успешным, на него приходиться 91% атак.

Клон фишинг – это фишинг, при котором используются оригинальные письма. Мошенник получает письмо организации, которое имеет вложение или ссылку и адреса получателей и использует его для создания похожего письма. Вложения и ссылки заменятся на вредоносные, а затем отправляются получателям. Чаще всего используются для заражения компьютеров. Пользователи открывают вложения, потому что уверены, что это настоящие письма, так как письма от организации приходили к ним до этого.

Китобойный – этот вид фишинга направлен на непосредственных руководителей организации или главных менеджеров. В этом случает электронное письмо или страница сайта будет иметь более представительский вид. Чаще всего данные письма содержат жалобу клиента, вызов в суд и тому подобное.

Защита от фишинга

Эксперты из «Лаборатория Касперского» предлагают следующие способы защиты от фишинга:

– Завести несколько адресов электронной почты. Рекомендуется завести минимум 2 адреса: первый – для личных сообщений, второй – «публичный». Личный адрес электронной почты использовать для личных сообщений. Чтобы защитить личный сайт, можно использовать следующие рекомендации:

– Никогда не публиковать личный адрес электронной почты на общедоступных интернет-ресурсах.

– Если личный адрес обнаружен злоумышленниками, его надо поменять. Это поможет избежать получения спама.

«Публичный» электронный адрес использовать для регистрации на форумах и в чатах, а также для подписки на почтовую рассылку и другое. Относится к данному адресу необходимо как к временному. Шансы, что мошенники перехватят адрес, используемый в открытом доступе, очень велики — особенно если он используется часто. Также можно завести несколько «публичных» адресов. Специалисты рекомендуют не отвечать на спам. Большинство спамеров фиксируют получение ответов. Рекомендуется заводить учетную запись для электронной почты

только у тех провайдеров, которые используют спам-фильтры. Выбирать антивирус, который имеет также расширенные функции защиты от спама.

УДК 004.056.53

Пенькова Инесса Вячеславовна
д.э.н., профессор
Кислинг Эльвира Сергеевна
магистрант
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЗНАЧЕНИЕ БЕЗОПАСНОСТИ САЙТА ДЛЯ МАРКЕТИНГОВОЙ КОМПАНИИ В ИНТЕРНЕТ

Сегодня сайт компании реализует не просто ее представление в среде Интернет, но становится источником бизнеса, каналом продаж и привлечения клиентов.

Наиболее распространённой проблемой является блокирование сайта антивирусом и поисковой системой (добавление в чёрный список), в результате чего компания несёт убытки, связанные с SEO (Search Engine Optimization), потому как за несколько дней кампания по продвижению сайта в поисковых системах не только перестаёт функционировать, но и наработанные результаты теряются. Поэтому, крайне важно обеспечить безопасность сайта.

Жертвой злоумышленников может стать любой хорошо продвигаемый сайт, который после взлома используется для распространения спама, вредоносного кода, нелегального контента или рекламы. Отметим, что поиск сайта для взлома происходит автоматически специальными программами, поэтому чем больше будет принято мер по обеспечению безопасности сайта, тем выше вероятность, что именно он попадёт в поле зрения злоумышленников.

Рассмотрим какую опасность несёт взлом сайта для маркетологов. В первую очередь пострадает бюджет, выделенный на SEO. Результаты, достигнутые с помощью SEO также утрачиваются, а именно: трафик снижается в разы; сайт закрывается для доступа; поисковые машины накладывают на сайт и его страницы «фильтры»; теряются позиции страниц в поисковом индексе; теряется доверие со стороны пользователей.

В случае атаки сайта злоумышленниками определяющую роль в будущей работе сайта играет время реагирования на проблему. В случае, когда сайт заражён вирусом и блокируется поисковыми системами, его возвращение в поисковую выдачу занимает достаточно длительное время. Подчеркнем, что сайты часто создаются на основе готовых платформ CMS (система управления контентом), это дешевле самостоятельного написания сайта. CMS уже изначально могут содержать уязвимости, которые устраняются во время обновлений систем, но новые угрозы также не перестают возникать.

Кроме вирусов сайт может быть использован как дорвей, т.е. страница сайта (или несколько страниц) оптимизируется для поисковых запросов и перенаправляет пользователей на другие сайты. В данном случае существует угроза исключения страниц сайта из индексирования и ранжирования или применения фильтра со стороны поисковых машин. Для решения такой проблемы необходимо удалить скрипты генерирующие дорвеи и в файле robots.txt запретить индексировать спам-страницы.

Для того, чтобы защитить сайт необходимо снижать риски взлома или заражения путем проведения диагностики и мониторинга сайта, обновления программного обеспечения и установки защиты.

Сервисы для веб-анализа предоставляют для пользователей функцию диагностики сайта, где можно проверить наличие вредоносного кода на страницах сайта или подозрительной активности (XSS, спам, скрытые спам-ссылки).

Таким образом, обеспечение и периодическая проверка уровня надёжности и безопасности сайта позволит снизить материальные и репутационные риски.

УДК 004.056.53

Пенькова Инесса Вячеславовна
д.э.н., профессор
Кучинская Анна Александровна
магистрант
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ВИРТУАЛЬНОМ ПРЕДПРИЯТИИ

В настоящее время виртуальные предприятия интенсивно развиваются, что обусловлено тем фактом, что общество находится на этапе социально–экономической формации, так называемого, информационного общества. Быстрое формирование экономики знаний, тотальная компьютеризация социума и развитие сети Интернет дает возможность развиваться виртуальным предприятиям. Вместе с расширением такого рода бизнеса появляются и риски, связанные с безопасностью, в первую очередь, с информационной защищенностью.

Информационная безопасность виртуального предприятия предполагает защищенность интересов предприятия от существующих или возможных угроз информационным ресурсам.

Основополагающей целью информационной безопасности является сокращение экономического и морального ущерба предприятия, связанного с повреждением или неправомерным использование информационных ресурсов. К информационным ресурсам (ИС), требующим защиты, относят:

технические средства автоматизации (компьютерная техника и средства связи);
электронные носители всех видов;
базы данных на различных, в том числе и на электронных, носителях;
архивы и библиотеки (электронные и машиночитаемые);
знания персонала.

Для того чтобы предупредить ущерб целесообразно принимать своевременные меры по защите ИС:

осуществление постоянного анализа возможных рисков;
совершенствование политики и стратегии информационной безопасности предприятия;
планирование обеспечения информационной безопасности.

Для обеспечения информационной безопасности следует выполнять следующие задачи:

выявлять и пресекать попытки уничтожения или фальсификации информации;
определять и прекращать возможную нелегальную модификацию данных;
обнаруживать и останавливать попытки несанкционированного получения информации;
ликвидировать последствия успешной реализации информационных угроз;
находить и нейтрализовать возможные или существующие каналов утечки информации;
нивелировать причины появления каналов утечки информации.

Таким образом, информационная безопасность виртуального предприятия обеспечивается комплексом мер по реализации и решению стратегических задач в соответствии с разработанным стратегическим планом.

УДК 004.055

Пенькова Инесса Вячеславовна
д.э.н., профессор
Серафимова Анастасия Александровна
студентка
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СЛУЖБЫ ДЛЯ РЕГИСТРАЦИИ ПРЕДПРИЯТИЙ ОНЛАЙН

В современных условиях хозяйствования весьма актуальным является вопрос о службах для регистраций предприятий онлайн, что требует теоретико-практического анализа.

Существует множество сервисов для он-лайн регистрации предпринимателей как электронной, так и офф-лайновой коммерческой деятельности.

Портал iGov поможет в регистрации предприятия. Все действия сводятся к заполнению заявки, в которой определяется сфера деятельности и условия налогообложения, после чего пользователь получает уведомление о постановке на учет и том, что его бизнес зарегистрирован.

Прежде чем начать регистрацию необходимо сформировать устав фирмы, который должен быть оформлен в соответствии с законодательством. Далее решается вопрос с юридическим адресом компании, определяется состав учредителей, размер уставного капитала и избирается директор, что подтверждается соответствующими выписками из протоколов заседания учредителей. Вся эта информация входит в пакет документов, предоставляемых на начальном этапе регистрации. Существует регистрационный портал, обеспечивающий электронную подачу всех необходимых документов для проведения государственной регистрации юридических и физических лиц.

Сервис 1С-Старт бесплатно поможет собрать все требуемые документы для создания соответствующего пакета. Данная служба предоставит возможность оформить и оплатить госпошлину и подать заявку в регистрационный орган. Сервис оснащен доступной и понятной информацией, консультанты помогают систематизировать часто задаваемые вопросы и дают на них четкие ответы.

Данный портал предполагает порядок создания и регистрации предприятия, а именно:

устав компании;

решение о создании фирмы;

заявление по форме Р11001;

документ об оплате государственной пошлины.

Если начальный этап пройден успешно, то на следующем шаге необходимо:

получить в ИФНС выписки о государственной регистрации;

заказать изготовление печати;

открыть расчетный счет;

поставить фирму на учет в пенсионном фонде, фондах медицинского и социального страхования.

Подводя итог, отметим, что службы для регистрации предприятий онлайн, сокращают время работы, удобны в использовании, что является серьезным преимуществом предоставляемого онлайн сервиса.

УДК 681.3.06

Попов Виталий Борисович
к.ф.-м.н., доцент
Кобзарь Никита Сергеевич
студент
Институт экономики и управления
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Республика Крым, Россия

ПЕРСОНАЛИЗАЦИЯ СТРУКТУРЫ ВЕБ-САЙТА НА ОСНОВЕ МЕТОДОВ НЕЛИНЕЙНОЙ КЛАСТЕРИЗАЦИИ

Актуальность работы. В электронной коммерции целью создания сайта всегда является получение дохода. Чем выше посещаемость, и чем дольше пользователь находится на сайте, тем больше доход. В связи со стремительным развитием методов и алгоритмов поисковых систем привлечение клиентов на сайт является важной и сложной задачей. Не менее важными задачами являются следующие: как заинтересовать пользователя, чтобы он больше времени провёл на сайте; как из посетителя сделать потенциального клиента; как вернуть пользователя на сайт; как привлечь больше потенциальных клиентов.

Целью данной работы является изучение и разработка новых методов персонализации структуры веб-сайта на основе методов нелинейной кластеризации для решения вышеперечисленных задач.

Основной материал. Главная задача владельца какого-либо сайта – увеличение процента конверсии. Примем следующие определения.

Определение. Конверсия в интернет-маркетинге – это отношение количества посетителей, совершивших какие-то целевые действия на сайте (покупка, регистрация, подписка, посещение какой-либо страницы сайта, переход по рекламной ссылке), к суммарному числу посетителей, определенное в процентах.

Многообразие сайтов породило ужесточение требований, которые предъявляют пользователи к посещаемым сайтам. Зачастую, если пользователь в течении некоторого времени не обнаруживает того, что ищет, то он переходит на другой ресурс. Решением ситуации, когда становится сложно создать запоминающийся и уникальный сайт, является персонализация сайта.

Определение. Персонализация сайта – это комплекс маркетинговых и технических мер, направленных на адаптацию внешнего вида и контента сайта под разные категории посетителей. Если каждой категории посетителей сайта будет предоставляться персонализированный контент, то можно существенно повысить эффективность сайта.

Персонализация страниц сайта позволяет значительно поменять отношение посетителей. Благодаря чему не только посетитель будет обращаться к сайту, но и сайт будет обращаться к каждому посетителю персонально, как к имеющему личные интересы.

После каждого посещения сайт заносит в базу данных информацию о каждом пользователе и о каждом действии, которое совершают пользователи. И при каждом следующем посещении пользователем, который был на этом сайте раньше, сайт будет подстраиваться под его интересы.

При посещении не персонализированного сайта, все посетители видят общую одинаковую информацию, общие и одинаковые специальные предложения или акции.

Исходя из статистики, внедрение подобной системы значительно увеличивает процент конверсии. В результате этого увеличивается количество посещений и продаж.

Российские интернет-магазины используют два основных вида инструментов персонализации сайта:

1. *Индивидуальные продажи – скидки, акции и специальные предложения конкретным сегментам пользователей.*

Система анализирует посетителей сайта, получает демографические и поведенческие данные. На основе этой информации потенциальному клиенту отображается персональное предложение. К примеру, предоставляются купоны или скидки на товары, которые он просматривал.

2. *Персонализация товарных предпочтений на сайте и в почтовых рассылках*

В данном случае контент сайта изменяется в соответствии с товарными предпочтениями посетителя. Например, пользователю отображаются товарные рекомендации следующего вида: самые популярные товары в интернет-магазине; товары, схожие с просматриваемыми пользователем; рекомендации поисковой системы и т.д.

E-mail рассылку используют, если выполняются заданные администратором условия.

Например, если пользователь:

- Закрывает сайт с товарами в корзине.
- Закрывает сайт, просмотрев какие-либо товары.
- Покупает товар и т.д.

Для владельцев и маркетологов интернет-магазинов актуальной задачей является достижение наибольшего количества сделанных заказов. На отечественном рынке электронной коммерции в настоящее время недостаточно заказать дизайн, внедрить адаптивную верстку, нанять онлайн-оператора. Для того, чтобы сайт был конкурентоспособным и имел успех, необходимо заняться персонализацией сайта.

УДК 65.011

Попов Виталий Борисович
доцент, к.ф.-м.н.
Федосеева Карина Николаевна
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ КОНТЕНТОМ WEB-САЙТА

Актуальность работы. Безопасность сайта является важнейшей частью его качественной работы и Web-программирования в целом.

В большинстве своем современные Web-сайты представляют собой не статический набор HTML-страниц, но динамически генерируемую информационную структуру. В качестве такого

контент-генератора используются системы управления контентом – Content Management Systems (CMS) или более точно Web-content Management Systems.

Целью данной работы является анализ существующих методов информационной защиты систем управления контентом современного Web-сайта, а также разработка модели персонализации веб-сайта, способной обеспечить эффективный доступ пользователей к релевантной информации на всех этапах интерактивного сеанса. Здесь под эффективностью персонализации, а также доступа к релевантной информации будем понимать точность сформированных системой персонализации информационных рекомендаций.

Системы управления контентом web-сайта. Следующие утверждения характеризуют систему управления Web-контентом (Web-content Management Systems).

- Системы управления Web-контентом представляют собой программное обеспечение (инструменты Web-программирования), позволяющее проектировать, разрабатывать и поддерживать динамические информационные Web-сайты.
- Преимущество динамических сайтов заключается в отделении дизайна от информационного наполнения, что в свою очередь позволяет автоматизировать документооборот, бизнес-процессы, механизмы персонализации.
- Системы управления Web-контентом снижают время разработки, стоимость создания и поддержки сложных Web-сайтов.
- Основными функциями систем являются разработка контента, управление сайтом, доставка контента.
- В основе систем управления Web-контентом лежит трехуровневая архитектура клиент/Web-сервер/сервер приложений (*three-layer*), что облегчает работу клиентов и доступ к информации

Блоки контента, из которых динамически строится итоговая страница, хранятся в базе данных Web-ресурса. С одной стороны, это облегчает работу с сайтом и его контентом, с другой стороны – создает множество проблем с точки зрения информационной безопасности. Со стороны разработчика чтобы обезопасить систему управления сайтом, при написании кода CMS-системы используется несколько алгоритмов. Наиболее распространенным и оптимальным является алгоритм, придерживающийся определенной архитектуры безопасности, которая выглядит следующим образом: единая система входа и авторизации; для каждого пользователя имеется одинаковый бюджет; разграничение прав доступа по уровням; обязательно шифрование информации при получении и передаче во внешнюю среду; постоянное обновление системы; функция ведения журнала отчетности; соблюдение политики работы с переменными и внешними данными; использование метода учета и контроля за критически опасными участками кода системы. Существующие правила и методы позволяют значительно снизить вероятность взлома системы и сайта соответственно, даже при наличии некоторых уязвимостей в программной части сайта

УДК 004.056

Рыбников Андрей Михайлович,
к.э.н., доцент,
Рыбников Михаил Сергеевич,
к.ф.-м.н., доцент,
Валеса Никита,
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

В основу системы мгновенного обмена сообщениями входит моментальная доставка сообщений от адресата к получателю, используя Интернет. Преимущественно система акцентирована на двух участников: может передаваться текстовая информация, голосовые сигналы, рисунки, видеоматериал, создаваться коллективная беседа, в которой можно рисовать или играть в игры. Почти все приложения-мессенджеры на сегодняшний день могут использовать систему конференций, то есть разговор или видео звонок сразу нескольким пользователям.

Как правило, мессенджеры не функционируют независимо, а подсоединяются к центральному компьютеру сети обмена сообщениями, то есть к серверу. По этой причине мессенджеры и называют клиентами (клиентскими программами). Название считается понятием из клиент-серверных технологий.

Широкому диапазону пользователей известно определенное число популярных сетей (и клиентов) обмена сообщениями, таких как IRC, QIP, Skype, ooVoo, AIM, Bingoo, ICQ, RedPhone, MSN, Yahoo!, Jitsi, XMPP. Каждая созданная программа обладает отдельным сервером и протоколами, определяющими уровень безопасности, отличается собственными инструкциями и спецификами.

Между разными сетями, как правило, нет прямой связи (лишь в XMPP имеется понятие межсетевого подключения), к примеру, пользователь сети Skype не может установить связь с пользователем сети ICQ, но он может быть одновременно пользователем двух или более сетей.

Почти каждая команда разработчиков в определенной сети создает свой мессенджер. Некоторые программы, созданные разработчиками подобных сетей: ICQ, WindowsLiveMessenger, Yahoo! Messenger, а также Skype.

Таким образом, если один из адресатов использует только сеть ICQ, а другой – сеть MSN, то возможно обмениваться с ним информацией одновременно, установив на своем компьютере либо смартфоне и ICQ, и MSN Messenger и завести личный аккаунт в обеих сетях (либо через соответствующие сети в XMPP).

В качестве дополнительного мессенджера можно использовать программу стороннего изготовителя, как платную, так и бесплатную. Известными альтернативными программами для обмена информацией в сети ICQ являются QIP 2005/QIP Infium, Psi/Psi+ (через XMPP-транспорт), Trillian, Miranda IM, Pidgin, MyChat.

Также некоторые из них дают возможность присоединяться сразу к нескольким сетям, то есть являются мультипротокольными, что избавляет от необходимости скачивать и устанавливать дополнительный мессенджер для каждой сети и позволяет обмениваться информацией со всеми адресатами одним способом, независимо от сети; все приведённые в предыдущем предложении версии ICQ, за исключением версии QIP 2005, поддерживают протокол XMPP.

Большинство IM-сетей задействуют скрытые протоколы, потому альтернативные клиенты могут владеть уменьшенным наборов стандартных функций, чем официальные, но на практике обычно выходит наоборот.

Однако при модификациях протокола на стороне сервера сети альтернативные клиенты могут неожиданно прекратить функционировать (к примеру, такое проявление отслеживалось для «нефирменных» клиентов обслуживания ICQ в Российской Федерации).

В виде альтернативы проприетарным протоколам для IM был сконструирован публичный и хорошо расширяемый протокол XMPP (еще известный как Jabber), применяемый в подобных сервисах, как GoogleTalk, Я.Он-лайн и др.

Данный протокол чаще всего используется для организации общения в объединенных и других локальных сетях и обладает рядом существенных плюсов, как, например, шифрование текстовых сообщений и стабильность работы на неустойчивых каналах связи.

Протокол децентрализованный, его архитектура похожа на электронную почту, где есть возможность общения между пользователями, использующие аккаунты в разных серверах. Если обрывается работа одного сервера, то это не влияет на дееспособность всей сети.

УДК 004.056

Рыбников Андрей Михайлович,
к.э.н., доцент,
Рыбников Михаил Сергеевич,
к.ф.-м.н., доцент,
Зарицкий Александр,
студент
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, РФ

СКРЫТЫЕ ВОЗМОЖНОСТИ, ВЛИЯЮЩИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В МЕССЕНДЖЕРАХ

В процессе анализа выявлены скрытые возможности, которые увеличивают уровень приватности при использовании, в двух наиболее популярных мессенджерах в России, а именно: WhatsApp и Telegram. К таковым в *WhatsApp* относятся:

переписка на компьютере, настраиваемая путем посещения сайта web.whatsapp.com и запуска приложения на телефоне (в iPhone зайти в настройки, в Android — в меню), используя WhatsAppWeb необходимо отсканировать QR-код;

скрыть последнее посещение: Меню> Настройки> Аккаунт> Приватность>Отметить людей, которые могут знать, когда пользователь заходил последний раз в сеть;

не засорять память устройства фотографиями и видео: по умолчанию медиа из чатов загружаются в общую память смартфона, но эту функцию целесообразно отключать (Настройки> Чаты и звонки> Автозагрузка медиа >Убрать галочки с нужных пунктов);

отправить переписку на личную почту: перейти в нужную беседу> Меню> Еще> Отправить чат по почте;

отключить уведомления -перейти в нужную беседу>Нажать на имени контакта или группы>Выбрать «Не беспокоить» и установить срок игнорирования;

добавить избранный контакт на экран смартфона путем перехода в нужный диалог> Меню> Еще> Не беспокоить> Добавить ярлык;

установить индивидуальные оповещения на избранный контакты: Меню> Посмотреть контакт> Индивидуальные уведомления> Установить галочку и выбрать звук.

В мессенджере *Telegram* скрытые возможности обеспечения информационной безопасности можно свести к следующим:

скрыть отображение последнего визита в приложение: Settings>PrivacyandSecurity>LastSeen>. Выбрать того, от кого скрывается текущий статус сетевой активности;

повышение уровня защиты аккаунта пользователя с помощью такой процедуры: Settings>PrivacyandSecurity>. Подключить двухступенчатую аутентификацию через вспомогательный пароль, восстановление которого привязывается к email-адресу. В этом же меню устанавливается и получается цифровой пропуск, который приложение вручную закрывает на замок;

фильтр потока скачиваемых файлов: Settings>ChatSettings–CacheSettings>. Подобрать опцию, чтобы файлы, к которым не обращались более недели, автоматически стирались с кэша программы. В случае экстренной необходимости, всегда можно найти это в переписке и вновь загрузить с облака Telegram, либо сохранить в облако или же на мобильный телефон;

добавление стикеров других пользователей, если пользователю понравился набор стикеров в переписке, необходимо нажать и удерживать сам стикер и выбрать Info>AddStickers, тем самым добавив весь набор стикеров в память устройства;

создание и использование секретных чатов: SecretChats – самоуничтожающиеся сообщения с высокой степенью безопасности, которые не сохраняются на сервере Telegram и не будут доступны к использованию сразу же после того, как пользователь сменит устройство или выйдет из приложения;

массовая рассылка общего сообщения (индивиду) –при отправке массовой рассылки одного сообщения с соблюдением анонимности получателей друг для друга используется функция Трансляции (Broadcasts);

структурный вид диалогов: в длительной переписке, в особенности групповой, легко запутаться. Есть ряд нужных функций, для того чтобы структурировать переписку: отвечать на определенное сообщение, нажав на нем и выбрав Reply, назначать через символ @ упоминания определенных людей, которым адресуется письмо, либо создавать знаком # хештеги для различных типов сообщений, для того чтобы ускорить поиск по ним.

Подводя итог, отметим, что Telegram является наиболее популярным в России, и. признан мировыми экспертами как «мессенджер высокой защиты SMS - сообщений». Высокий уровень популярности, отличный уровень защиты и бесплатный доступ к мессенджеру делают Telegram одним из наиболее используемых в России.

УДК[347.77/.78 : 004.77] : 005.922.1

Смирнова Оксана Юрьевна,
ассистент
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И.Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В СЕТИ ИНТЕРНЕТ

В информационном обществе различные объекты интеллектуальной собственности (ИС) используются в сети Интернет: объекты авторского права и смежных прав, коммерческие обозначения, результаты научно-технического творчества. Специфика юридической защиты прав: объекты ИС используются в сети, в качестве контента веб-сайтов (всевозможные данные) и доменных имен (торговые марки, фирменные наименования, географические обозначения). В настоящее время механизмами защиты прав ИС в сети Интернет является защита прав в судебном порядке, в административно-правовом порядке, самозащита прав. Способы защиты прав ИС в сети Интернет определены, спецификой информационного пространства: формой, способами и территорией распространения информации, скоростью обмена данными, ограниченным доступом к информации, владельцем веб-ресурса или личности, которая разместила неправомерный контент. Специфика информационного пространства сказывается на особенностях базы доказательств правонарушений в сети и группе участников спора. Интернет - площадка, позволяющая открыто обмениваться объектами авторского права. В качестве содержимого веб-сайтов можно использовать:

- литературные и художественные труды,
- музыку,
- видеоролики, видеофильмы,
- компьютерные программы,
- фотографии,
- базы данных.

Размещение объекта авторского права на веб-сайте без согласия автора является нарушением авторского права и предоставляет основания для защиты интересов правообладателя – главный принцип защиты прав в сети. Применение принципа защиты прав в сети на практике связано с различными сложностями, такими как: установление личности правонарушителя, который должен нести ответственность за не правомерные действия (у правообладателя должна быть возможность исполнить решение суда, или обратиться к другим мерам прекращения нарушения). В законодательстве о телекоммуникациях, написано, что группа отвечающих за “контентные” нарушения состоит из потребителей телекоммуникационных услуг, операторов и провайдеров телекоммуникаций, а также собственников веб-сайтов. За нарушение авторских прав в сети отвечают: личность, которая распространила неправомерный контент, собственник веб-сайта. В случае если личность правонарушителя не установлена, информация является анонимной, свободный доступ к сайту, нарушителем является собственник веб-сайта, с размещенной информацией (создание технологических возможностей и условий для распространения информации являющейся ИС). Эта концепция касается практики рассмотрения дел о защите чести, достоинства и репутации физических и юридических лиц и применяется в делах о нарушении авторских прав в сети Интернет. Провайдеры и операторы телекоммуникаций не несут ответственности:

- за действия пользователей во время хостинга, если прекратили размещение и доступ к информации;
- за содержание информации, предающейся с помощью сетей (не имеют прав контролировать ее контент);
- за различные товары, информации и услуги, которые предоставлены с помощью сети.

Также существует проблема ответственности за нарушение прав на торговые марки (ТМ):

- в доменных именах;
- на веб-страницах;
- в баннерной рекламе;
- в мета-тегах,
- в гиперссылках.

Привлечь к ответственности правонарушителя в доменной зоне и за неправомерное использование ТМ практически невозможно, т.к. сложно установить правонарушителя (данная информация предоставляется по запросу правоохранительных органов или суда, только суд может обязать киберсквоттеров прекратить использование ТМ в имени домена).

К сожалению, законодательство, судебная система, правила использования доменов не нашли грамотного решения этих проблем. Следовательно, дела связанные с противодействием захвата доменных имен, требуют дальнейшего анализа и стратегической разработки защиты прав ИС. Ответственность участников правоотношений в сети остается открытой проблемой, требующей принятия единственного верного решения. Правообладатели, выкладывая свою ИС в просторы Интернета рассчитывают на то, что их права эксклюзивны, но повсеместное онлайн использование объектов ИС подразумевает наличие рисков, которые полностью устранить не возможно. Установление приемлемого равновесия в правовых отношениях между правообладателями ИС и объектами, которые ее используют, является важнейшей проблемой:

- на законодательном уровне,
- на правоприменительном уровне,
- на уровне саморегуляции Интернет-сообщества.

УДК 004.7.056.53

Солдатов Максим Александрович
к.ф.-м.н., доцент
Солдатова Светлана Александровна
старший преподаватель
Таштанова Лидия Лативицевна
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Обеспечение безопасности web-приложений – сложная многоуровневая задача, имеющая большое количество аспектов, как одинаковых для любых сетевых служб, так и свойственных исключительно для web-приложений. Первые включают безопасность сетевой инфраструктуры (брандмауэров, маршрутизаторов, DNS серверов и т.п.), безопасность физических серверов, на которых располагаются web-сервер и БД, включая безопасность реализации стека протоколов TCP/IP и других функционирующих сервисов и т.д. Специфическими для web-приложения аспектами являются безопасность web-сервера и его конфигурации как сервиса и непосредственно безопасность скриптов, реализующих основную функциональность.

Среди потенциальных угроз безопасности безопасности web-приложений можно выделить: 1) неавторизованное чтение данных из нашей базы; 2) нарушение функционирования приложения, или DoS (Denial of Service) атака; 3) неавторизованная модификация данных в нашей базе; 4) запуск посторонних процессов или модификация файлов на сервере; 5) чтение файлов на сервере.

Большинство атак на web-приложения осуществляется специальным выбором параметров, передаваемых скрипту. Главный метод защиты от такой угрозы основывается на тщательной проверке всех без исключения данных, которые получаются от пользователя перед их использованием в программе. Одним из самых распространенных способов реализации угроз 1 и 2 является «SQL injection», т.е. посылка скрипту данных, сформированных с целью выполнения скриптом SQL запроса, отличающегося от предусмотренного автором скрипта.

Необходимые проверки пришедших от пользователя данных в остальных случаях зависят от специфики использования этих данных. Частой практикой является работа с файловой системой с именами файлов, задаемыми пользователями. В такой ситуации для обеспечения необходимого уровня безопасности необходима весьма строгая проверка информации по средствам регулярных выражений. Наиболее простым и надежным методом является замена пользовательских имен файлов на сконструированные заведомо безопасные имена и хранение в БД таблицы соответствия этих имен. Второй метод заключается в жестком ограничении набора допустимых символов в задаваемых именах файлов (концепция «белых списков», т.е. разрешено лишь то, что заранее обозначено). Как правило неопытные программисты используют концепцию «черных списков», т.е. обнаруживают известные потенциально опасные

конструкции. Данный подход является более громоздким и позволяет большую вероятность появления уязвимостей, т.к. при работе с файловой системой по средствам системной функции open, Perl гарантирует ее высокую гибкость за счет разнообразия допустимых синтаксисов вызова. Т.о. функция может запускать другие программы и объединять их конвейерным механизмом передачи информации, копировать файловые дескрипторы и выполнять множество других потенциально опасных (в случае их непредусмотренного заранее вызова) операций. Тщательное и полное предотвращение различных типов нецелевого использования подобных функций работы с файлами, сокращая при этом возлагаемые на имена файлов ограничения является достаточно трудной задачей.

Еще одной из постоянно встречающихся ситуаций является потребность предоставлять пользователям данные, поставленные другими пользователями (например, гостевые книги форумы и др.). Основная проблема в данном случае заключается в том, что злонамеренный пользователь может ввести такие данные (например, программу на языке JavaScript), которые отрицательно отразится на других пользователях web-ресурса. В качестве сравнительно безопасного примера можно привести возможность быстрого закрытия только что открытой страницы. Чтобы решить эту проблему используют концепции подмены настоящих тэгов их искусственными субститутами, черных списков и белых списков. Так же как и в предыдущей ситуации, черные списки будут являться самым ненадежным и самым трудоемким сценарием действий.

Другие возможные слабые стороны в обеспечении безопасности web-приложений включают вызовы дополнительных скриптов, не предназначенных для прямой работы с пользователями, попытки чтения файлов, которые содержат скрытые данные сервера и др. В качестве защиты от таких действий выступает правильное распределение данных между скриптами и расположение скриптов на сервере.

Так же следует отметить, что одним из важных принципов обеспечения безопасности web-приложений является сведение к минимуму данных о внутренней архитектуре системы, которые доступны пользователям. Например, в сообщениях об ошибках при работе скрипта не стоит сообщать пользователю текст SQL запроса, вызвавшего ошибку, т.о. информация о структуре расположения данных в СУБД может облегчить злоумышленнику последующее планирование атаки.

УДК 004.056.5

Бойченко Олег Валерьевич,
д.т.н., профессор,
Гавриков Илья Владимирович,
студент 2-го курса бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ ПРОДУКТОВ MDM ДЛЯ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ В КОРПОРАТИВНОМ СЕКТОРЕ

Сегодня повышение мобильности рабочей силы в корпорациях является одним из главных направлений их развития.

В опросе 2015 года с участием более 1300 респондентов, корпоративная мобильность была на втором месте по важности среди ИТ-инициатив предприятий, уступив только консолидации дата-центров.

По оценкам экспертов, доля рынка BYOD и корпоративной мобильности вырастет с 35,1 млрд долларов в 2016 году до 73,3 млрд долларов в 2021 с ежегодным темпом роста в 15,87%.

Повышение мобильности происходит в первую очередь за счёт интеграции мобильных устройств в рабочий цикл компании.

Однако работа с мобильными устройствами в корпоративном контексте подразумевает определённые, а зачастую и достаточно серьёзные, риски, связанные с безопасностью информации.

Как и любое устройство, мобильные телефоны и планшеты подвержены риску утечки информации и взлома.

Так, в течение 4 месяцев продукты мобильной безопасности компании Mobilisafe регистрировали уже ранее существовавшие, а также новые уязвимости в мобильных устройствах. Во время исследования было проанализировано более 134 уязвимостей в операционных системах и приложениях.

В ходе исследования было выяснено, что все чаще уязвимости в приложениях и операционных системах эксплуатируются для «компрометации моделей безопасности, защищающих данные компании».

Согласно данным исследования, 71% устройств содержали уязвимости высокой степени опасности в операционных системах и приложениях. При этом, 38 различных версий операционных систем содержали уязвимости высокой степени опасности.

Исследователи компании отметили, что количество устройств, содержащих уязвимости, уменьшилось бы в 4 раза, если бы программное обеспечение этих устройства своевременно обновлялось до последней версии.

Ситуацию обостряет проблема, связанная с результатами исследования экспертов IBM X-Force, который свидетельствуют о быстром изменении общей ситуации с информационной безопасностью в части мобильных устройств, характеризуется хорошо спланированными, мощными и широкомасштабными атаками, растущим числом уязвимостей защиты мобильных устройств, а также появлению более изощренных угрозам, таким, например, как «вейлинг», являющейся разновидностью фишинговой атаки, осуществляемой по методу «spear phishing» (когда злоумышленник обманом заставляет пользователей раскрывать свои пароли).

Кроме того, исследования показывают, что вероятность утечки и взлома можно понизить, проведя обучение персонала правильному поведению с мобильными устройствами и сетями, однако даже в идеальном сценарии это не исключает риска нарушения информационной безопасности полностью, так как доля человеческого фактора является превалирующей в спектре угроз информационной безопасности (эксперты заключают, что только 1 из 10 инцидентов, связанных с информационной безопасностью, относится в целенаправленным действиям внешних злоумышленников, остальные же (9) являются определяющими в отношении внутренних уязвимостей, связанных с неправомерными действиями персонала организации).

Одной из важнейших мер для дополнительной безопасности мобильных устройств, используемых в корпоративном контексте, является внедрение системы MDM.

Согласно результатам опроса 882 ИТ-профессионалов в корпоративной сфере, по состоянию на 2016 год 43% организаций используют решения MDM.

MDM (mobile device management, англ. управление мобильными устройствами) — набор технологий, позволяющих корпорации установить более жёсткий контроль над мобильными устройствами.

Сегодня на рынке существует значительное количество MDM-продуктов, различающихся между собой различными комбинациями используемых технологий и подходов к обеспечению информационной безопасности подконтрольных устройств.

Можно выделить следующие основные элементы корпоративной ИТ-структуры, диктующие выбор MDM-продуктов:

1. Внедрение политики BYOD. Bring your own device («возьми своё личное устройство») — корпоративная политика, позволяющая использовать персональные устройства в рабочих целях.

Если на предприятии внедрена BYOD-политика, то при выборе MDM-продукта необходимо исходить из соображений интеграции с существующей экосистемой устройства и разделением персональных и конфиденциальных корпоративных данных.

2. Локальный или облачный MDM. Как и многие программные продукты, многие MDM-системы сегодня переходят в облачный формат, и корпорация, желающая внедрить MDM-систему, должна взвесить плюсы и минусы облачных и локальных решений и сделать выбор.

Облачные решения обладают бесспорным преимуществом в плане простоты установки и использования, однако многие предприятия предпочитают иметь полный и единоличный контроль над своими конфиденциальными данными, храня данные на собственных серверах.

3. Контейнеризация. Идеология контейнеризации подразумевает под собой хранение всех конфиденциальных данных в специальном безопасном контейнере, доступ к которому возможен только с использованием узкого ряда специализированных приложений.

Это значительно затрудняет доступ к конфиденциальной информации для злоумышленников, но и делает работу с этой информацией для сотрудников менее комфортной.

С другой стороны, бесконтейнерные MDM-решения не хранят информацию таким образом, полагаясь вместо этого на средства удалённой очистки устройств от конфиденциальной информации. Использование таких MDM-продуктов позволяет сотрудникам использовать различные знакомые им приложения для корпоративных целей.

В заключение можно сказать, что все перечисленные выше варианты MDM-технологий имеют место в различных корпоративных контекстах, и выбор конкретного решения будет зависеть как от различных факторов корпоративной структуры, так и от других переменных, в том числе финансовых.

Для грамотного внедрения мобильных устройств в экосистему предприятия необходимо привлечение специалистов в данной сфере и обучения ИТ-специалистов работы с новой категорией устройств, а значит и новой категорией перспектив и рисков.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Солдатов Александр Николаевич
магистрант
Таврическая академия, факультет математики и информатики
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ СИСТЕМАХ

В настоящее время практически каждый человек является владельцем смартфона или планшета. Эти устройства настолько прочно заняли свою нишу в нашей повседневной жизни, что довольно сложно представить мир без них. А все благодаря широкому спектру выполняемых ими задач. Теперь это не только лишь средства связи, а еще почтовые ящики, навигаторы, фотоаппараты, органайзеры и т.д. Это лишь малая часть их богатого арсенала возможностей. В силу обстоятельств, эти устройства стали информационным хранилищем, изобилующим персональными данными о своем владельце. И речь идет не только о контактах из телефонной книги или компрометирующих фотографиях с последнего корпоратива, а, например, о паспортных данных человека либо номерах банковских счетов. Сразу же назревает вопрос: «А есть ли во всей этой среде слабые места и насколько они уязвимы?»

Несомненно, угрозы существуют, а количество их не так мало, как этого хотелось бы. На сегодняшний день на рынке гаджетов чаще всего встречаются устройства под управлением IOS, Android и Windows. Самыми популярными, благодаря своей ценовой политике, являются Android-устройсва, однако все исходные коды системы доступны и любой изъян мгновенно становится достоянием общественности. С продукцией Apple ситуация несколько иная. В силу закрытости системы, разработка вредоносных приложений более трудоемка и проблематична, но и цены на эти устройства выше, хотя это вовсе не мешает их популярности. С уровнем безопасности Windows все выглядит вроде бы безоблачно, но это для компьютерной версии системы. А вот в вариант для «младших» устройств перекочевала лишь часть средств защиты. Но в будущем ситуация может измениться в лучшую сторону.

Теперь о том, как вредоносные приложения попадают на устройства. Тут все предельно просто. В 99,9% случаев ответственность за заражение гаджета полностью ложится на своего владельца. Происходит это либо по неосторожности, либо по невнимательности или же глупости. Оставшаяся доля приходится на целенаправленное заражение устройства и при тщательном планировании оного, избежать его практически невозможно.

В завершение можно сказать, что все существующие ОС уже по умолчанию имеют довольно богатый набор средств защиты информации, такие как установка блокировки устройства, шифрование всех данных, слежка за поведением приложений и т.д., но большая часть из них владельцами не используется или же попросту отключается. Разработчики мобильных платформ регулярно выпускают обновления для своих продуктов, в которых помимо оптимизации работы системы также улучшается степень защиты устройств. Ко всему прочему не нужно пренебрегать специализированным программным обеспечением, таким как антивирусный монитор и сканер. При определенном желании, можно добиться довольно высокой степени защиты своего устройства, однако абсолютным его назвать вряд ли получится, т.к. с развитием средств защиты эволюционируют и способы ее обхода или взлома

УДК 004.056

Иванов Сергей Викторович,
к.ф.-м.н, доцент
Лукьянова Мария Альбертовна,
студентка
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

В последнее время все больше людей полагаются на мобильные приложения, поэтому их защищенность должна становится одним из главных приоритетов стратегии безопасности бизнес – процессов организаций и частных лиц.

Мобильное приложение – это компонент, который устанавливается на мобильное устройство, подключается к серверу мобильной телесистемы и управляет пользовательским интерфейсом и бизнес-логикой данного устройства.

Вместе с ростом популярности мобильных приложений, растет и их капиталоемкость, а вместе с этим и желание злоумышленников заполучить эти капиталы. Для этого существует множество различных способов, но с каждым годом разрабатывается все больше алгоритмов для противодействия этим угрозам.

Уникальное исследование оценки защищенности мобильных приложений, проведенное IBM X-Force, показало, что из тридцати, отобранных случайным образом, программ мобильных приложений четверть были вскрыты путем взлома (специалисты смогли узнать сохраненные на устройствах Pin-коды, номера кредитных карт), которые отнесли к небезопасным, а также в ряде случаев удалось получить несанкционированный доступ к истории платежей.

Эксперты аналитической компании Digital Security выделили несколько основных способов прорыва через системы безопасности мобильных приложений, к которым отнести: 1) манипуляции с каналами данных; 2) возможности скрытого внедрения SQL-операторов; 3) некорректные права доступа и многое другое. На данный момент большинство схем взлома ожидаемы, поэтому можно быть более или менее уверенным в защите своего мобильного устройства.

При проведении аудита безопасности клиентской части приложений на таких мобильных платформах, как Google Android, Apple iOS, Java, Windows Phone эксперты компании Digital Security выявили следующие типовые угрозы для мобильных приложений: 1) секретные данные в открытом виде; 2) небезопасные каналы передачи информации; 3) наличие отладочного кода; 4) внедрение SQL-операторов; 5) межсайтовый скриптинг (XSS); 6) отсутствие проверок входящих данных; 7) неправильная расстановка прав доступа; 8) слабая криптография.

По результатам исследования уязвимостей мобильных приложений, функционирующих под управлением iOS, Android и Windows Phone, проведенного компанией «Инфосистемы Джет», стало известно, что: 1) 98% программ имеют уязвимости; 2) 40% - обладают уязвимостями критического характера; 3) 22% (а это каждое пятое приложение) - используются незащищенные протоколы передач информации; 4) в 25% программ производится небезопасная аутентификация WEB-сервера; 5) в 87% - была выявлена недостаточная защита пакета приложения и его компонентов; 6) в 78% – отсутствие проверок наличия несанкционированного привилегированного доступа к мобильному устройству; 7) больше всего критичных уязвимостей было обнаружено в Android-приложениях; 8) меньше всего – в приложениях, работающих в среде iOS.

Оказывается, что все мобильные приложения содержат хотя бы одну уязвимость, которая позволяет перехватывать данные, которые передаются между клиентом и сервером.

Для защиты личной информации следует использовать криптографические возможности устройства, шифрование данных, удаленную очистку данных, а также необходимо регулярно проводить анализ защищенности приложения, с помощью которого можно определить утечку данных или неправильное использование шифрования.

УДК 004.056

Бойченко Олег Валерьевич
д.т.н., профессор,
Авдошин И. А.
магистрант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

ПОРЯДОК СОЗДАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Говоря о системах безопасности, нужно отметить, что они должны не только и не столько ограничивать допуск пользователей к информационным ресурсам, сколько определять и делегировать их полномочия в совместном решении задач, выявлять аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их последствия, гибко адаптируя структуру в условиях отказов, частичной потери или длительного блокирования ресурсов.

Не стоит, однако, забывать об экономической целесообразности применения тех или иных мер обеспечения безопасности информации, которые всегда должны быть адекватны существующим угрозам.

Создание комплексной системы защиты информации (КСЗИ) в информационно-телекоммуникационных системах (ИТС) осуществляется в соответствии с нормативным документом системы технической защиты информации на основании технического задания (далее – ТЗ), разработанным согласно требованиям нормативного документа системы технической защиты информации. Кроме того, при проектировании КСЗИ можно руководствоваться соответствующими стандартами.

Анализ исследований позволил установить, что в состав КСЗИ входят мероприятия и средства, которые реализуют способы, методы, механизмы защиты информации от:

- утечки техническими каналами, к которым относятся каналы побочных электромагнитных излучений и наводок, акустоэлектрических и других каналов;
- несанкционированных действий и несанкционированного доступа к информации, которые могут осуществляться путем подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоление мероприятий защиты с целью использования информации или навязывания ошибочной информации, применение закладных устройств или программ, использование компьютерных вирусов и т. п.;
- специального влияния на информацию, которое может осуществляться путем формирования полей и сигналов с целью нарушения целостности информации или разрушения системы защиты.

Для каждой конкретной ИТС состав, структура и требования к КСЗИ определяются свойствами обрабатываемой информации, классом автоматизированной системы (АС) и условиями ее эксплуатации.

В общем случае, последовательность и содержание научно-исследовательской разработки КСЗИ можно предварительно разделить на 4 этапа.

Несмотря на простоту структуры разработки КСЗИ, большинство организаций придерживается именно этого алгоритма. Однако данный алгоритм – это лишь основа проектирования. Каждый представленный этап отражает множество уровней в ходе проектирования, в зависимости от структуры АС требования, предъявляемых к ее системе защиты.

Так, для каждого типа угроз, возникающих при функционировании системы информационной безопасности, может быть одна или несколько мер противодействия.

В связи с неоднозначностью выбора мер противодействия необходим поиск некоторых критериев, в качестве которых могут быть использованы надежность обеспечения сохранности информации и стоимость реализации защиты.

При этом, принимаемая мера противодействия с экономической точки зрения будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного

экономического ущерба, превышает затраты на ее реализацию.

В этой ситуации можно определить максимально допустимые уровни риска в обеспечении сохранности информации и выбрать на этой основе одну или несколько экономически обоснованных мер противодействия, позволяющих снизить общий риск до такой степени, чтобы его величина была ниже максимально допустимого уровня.

Из этого следует, что потенциальный нарушитель, стремящийся рационально использовать предоставленные ему возможности, не будет тратить на выполнение угрозы больше, чем он ожидает выиграть.

Следовательно, необходимо поддерживать цену нарушения сохранности информации на уровне, превышающем ожидаемый выигрыш потенциального нарушителя.

Утверждается, что большинство разработчиков средств вычислительной техники рассматривает любой механизм аппаратной защиты как некоторые дополнительные затраты с желанием за их счет снизить общие расходы.

При решении на уровне руководителя проекта вопроса о разработке аппаратных средств защиты необходимо учитывать соотношение затрат на реализацию процедуры и достигаемого уровня обеспечения сохранности информации.

Поэтому разработчику нужна некоторая формула, связывающая уровень защиты и затраты на ее реализацию, которая позволяла бы определить затраты на разработку потребных аппаратных средств, необходимых для создания заранее определенного уровня защиты.

В общем виде такую зависимость можно задать исходя из следующих соображений: «Так, если определять накладные расходы, связанные с защитой, как отношение количества использования некоторого ресурса механизмом управления доступом к общему количеству использования этого ресурса, то применение экономических рычагов управления доступом даст накладные расходы, приближающиеся к нулю».

УДК 004.01.04

Бойченко Олег Валерьевич
д.т.н., профессор,
Тупота Елена Сергеевна
студентка бакалавриата
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРАВОВЫЕ АСПЕКТЫ ВНЕДРЕНИЯ СИСТЕМ ТИПА DATA LEAK PREVENTION НА ПРЕДПРИЯТИЯХ РОССИЙСКОЙ ФЕДЕРАЦИИ

Введение. При ведении любой коммерческой деятельности на данном этапе развития современного общества важнейшим аспектом является информация. Потеря данных является критичной для фирмы, это может привести к потере клиентской базы предприятия. На рынке для решения данной проблемы существует DLP (Data Leak Prevention) системы.

Постановка проблемы. DLP-технологии предотвращают утечку конфиденциальной информации из информационной системы предприятия, они могут быть программные или программно-аппаратными. Данные системы строятся на анализе потока данных, которые функционируют внутри ИС.

Однако существует правовой аспект внедрения DLP систем на предприятиях. При внедрении очень важным является полное обеспечение функционирования системы в рамках правового поля.

Целью данного исследования является изучение проблематики правовых аспектов при внедрении DLP систем на предприятиях.

Методы исследования. Информационная безопасность является ключевым аспектом в деятельности предприятия. Риски, связанные с утечкой данных влияют на ее привлекательность для инвесторов и клиентов. Вероятность утечки информации по вине сотрудников компании выше, чем утечка данных по причине внешнего вмешательства (взлома).

Практика показывает превышение внутренних утечек информации над внешними утечками в диапазоне 15-20%. При этом, по результатам анализа использования сетевых технологий в управлении предприятием, наиболее частыми причинами внутренних утечек является ошибочность в действиях пользователя сетевого ресурса при организации передачи данных.

Так, сотрудник может по ошибке отправить информацию не тому адресату. В такой ситуации для обнаружения несанкционированной передачи конфиденциальных данных не тому кругу лиц, на предприятиях наиболее целесообразно применять DLP системы защиты информации.

Основная задача DLP систем – мониторинг, идентификация и защита. Более подробно DLP технологии могут быть описаны как системы предотвращения утечек конфиденциальной информации из автоматизированной информационной системы вовне, а также программные или программно-технические технические устройства для такого предотвращения утечек. Особенностью DLP-систем является построение их архитектуры на анализе потоков данных, пересекающих периметр защищаемой информационной системы.

При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется. Распознавание конфиденциальной информации в DLP-системах производится путем анализа формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний, а второй позволяет выявить пересылку конфиденциальной информации во всем информационном потоке.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста, при чем сетевые компоненты контролируют трафик, пересекающий границы информационной системы.

Обычно система должна обеспечивать защиту на следующих каналах утечек:

- Внешние устройства;
- Информация находящаяся в сетевом доступе;
- Средства сетевой печати;
- Веб-ресурсы;
- Передача файлов по каналам HTTP, HTTTPS, FTP;
- Электронная почта;
- Программы взаимодействия с клиентами.

В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. Необходимость их использования стала упоминаться в стандартах и нормативных документах (например, раздел "12.5.4 Утечка информации" в стандарте ГОСТ ISO/IEC 17799-2005).

Для обеспечения сохранности персональных данных на предприятии существует ст. 10 ч. 4 ФЗ РФ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», данная статья дает право осуществлять контроль над каналами связи, по которым проходит информация имеющую коммерческую тайну.

Так же, для более глубокого контроля работодателем может быть применен Закон РФ от 21.7.3 №5485-1 "О государственной тайне", ФЗ от 27.07.06 № 149-ФЗ "Об информации, информационных технологиях и защите информации", ФЗ 27.07.06 № 152-ФЗ "О персональных данных".

Результаты исследования. То есть, в соответствии с законодательной базой необходимо персональное соглашение от каждого сотрудника, рабочее место которого подключено к системе о разрешении обработки персональных данных. Следовательно, корректное функционирование DLP системы в рамках правового поля Российской Федерации необходимо соблюдать все вышеперечисленные аспекты и законы.

Выводы. Таким образом, в ходе исследования нами были выявлены основные правовые особенности внедрения DLP систем на предприятиях. Для этого необходимо создать перечень сведений, которые составляют коммерческую тайну предприятия и не подлежат разглашению, и ознакомить с данным документом всех сотрудников организации, все сотрудники так же должны подписать документ запрещающий использование рабочих станций в личных целях.

Выработанный комплекс может помочь внедрить систему DLP, которая соответствовала бы полностью правовому полю Российской Федерации.

УДК 004.7.056.53

Воробьев Владимир Иванович
г.н.с., д.т.н., профессор
Монахова Татьяна Вячеславовна
соискатель
Санкт-Петербургский институт
информатики и автоматизации Российской академии наук
Санкт-Петербург, Россия

МЕТАМОДЕЛЬ ЗАЩИТЫ МЕТАДАННЫХ

Уязвимости в обработке метаданных ещё недостаточно исследованы, хотя современные инструменты автоматизации работы с базами данных, Data Mining, Big data, Semantic Web частично включают средства защиты метаданных. В условиях гигантского возрастания объемов информации (данные почти удваиваются ежегодно) метаданные получат всё большее значение как средство описания и самоописания данных и как средство интерпретации результатов измерений и моделирования. В будущем неизбежно возникнут новые или будут обнаружены уже существующие уязвимости, которые необходимо учитывать при конструировании средств защиты.

Эта информация сама по себе конфиденциальная, или относящаяся к коммерческой тайне, и в большинстве случаев имеет большее значение, чем сами данные, т.к. усвоение данных системами обработки невозможно без использования мета описания данных. В состав наиболее распространенных метаданных входят: адреса электронной почты, имена файлов, форматы данных, пути к файлам, характеристики системы создания или обработки данных, информация об авторах и ПО, и о платформах. К типам документов, содержащих метаданные, относятся документы DOC, DOCX, RTF, PDF, HTML, XML, для изображений - созданные или обработанные различными редакторами растровой графики файлы BMP, GIF, PNG и JPEG, аудио файлы MP3, веб-страницы, электронные письма, получившие массовое распространение форматы, используемые на различных сайтах в повседневной деятельности.

Структура и состав метаданных зависят от типа, формы представления и способа использования самих данных, которые могут включать в себя имя автора документа, организацию, автора или фирму изготовителя программного или аппаратного средства, историю преобразования документа и т.д. В ряде случаев это может быть даже текст, входивший в документ, позже удаленный, но хранящийся в виде метаданных. Примером аппаратной метки может служить EXIF тэг, помещаемый в снимок в формате JPEG цифровыми камерами и несущий, среди прочих, такие данные как время и режим съёмки кадра. Другим примером аппаратного размещения метаданных (PC World и на SecurityLab.ru) является нанесение цветными лазерными принтерами метки на распечатке. Особенно важную роль метаданных играют комментарии разработчиков в исходном коде и в исполняемых файлах.

Известны инциденты с оглаской на международном уровне. В одном случае, это был документ, подписанный премьер-министром Великобритании Тони Блэром, удаленный из документа текст содержал конфиденциальную информацию. Для специалиста и заинтересованного человека метаданные позволяют раскрыть большое количество защищенной информации.

Предлагается использовать технологию метаописания объектов на базе XML, применяя её для целей сокрытия метаинформации. Предлагаемые решения позволяют создавать средства маскировки электронных документов, Web-страниц, электронной корреспонденции.

Обычная практика защиты метаданных строится на умалчивании метаданных, таких как имена файлов, тип файла, формат и т.д. Цель предлагаемой системы состоит в том, чтобы всесторонне запутать метаданные с использованием методов обфускации, трансформации XML –описания данных таким образом, чтобы, оставив программу использующую это описание в рабочем состоянии, затруднить или сделать невозможным декомпиляцию или реинжиниринг системы для последующего несанкционированного использования модулей системы.

Предлагается использовать при построении системы защиты мета данных онтологическую модель(метамодель), состоящую из трёх следующих компонентов: XML- описание данных , XML- описание мета данных, онтологические представления метаданных и свзанных с ними данных, которые предполагается реализовать в разрабатываемой системе. Такая модель позволяет разрабатывать двух барьерную систему защиты как больших, так и обычных данных

УДК 32.019.51

Гончарова Оксана Николаевна,
д.п.н., профессор
Балабанова Полина Анатольевна
магистрант
Таврическая академия
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ГОСУДАРСТВЕННАЯ СТРУКТУРА ЗАЩИТЫ ИНФОРМАЦИИ

На сегодняшний день, нет полной уверенности в мерах, применяемых к обеспечению конфиденциальности и безопасности субъектов, участвующих в процессах информационного взаимодействия, а также эти меры не гарантируют отсутствие взлома и утечки конфиденциальной информации.

К сожалению, компьютер, как средство, использующееся для решения различных экономических, социальных и технических проблем, так же является причиной появления не менее серьезных проблем. Одна из них это проблема информационной безопасности.

На сегодняшний день инновация системы обеспечения информационной безопасности юридических и физических лиц основывается на переходе от всеобщего скрытия конфиденциальных данных к обязательной защищенности особо важных данных, обеспечивающей:

-в сфере информатизации: конституционные права индивидуальных предпринимателей, государственных учреждений и физических лиц;

-должный уровень конфиденциальности для данной информации;

-безопасность систем информационных ресурсов.

Главная идея политики государства в данной сфере это понимание важности защиты всех информационных ресурсов и информационных технологий, безрассудное отношение к которым будет причиной причинения ущерба их владельцу, обладателю или иному лицу.

Структура и главные обязанности государственной системы защиты информации от ее кражи из технических ресурсов и формировании работ по защите информации выражены в «Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденном Постановлением Правительства от 15 сентября 1993 г. № 912-51».

Данным Приложением предполагается, что все действия по защите информации, перерабатываемой возможными техническими способами, являются результатом управленческой, научной и производственной деятельности физических и юридических лиц, и производятся в комплексе с иными мерами по обеспечению утвержденного федеральными законами «Об информации, информационных технологиях и о защите информации» и «О государственной тайне» совокупности мер по сохранности сведений, хранящих в себе государственную или служебную тайну.

Итак, главной идеей политики государства в данной сфере является понимание важности защиты всех информационных ресурсов и информационных технологий, безрассудное отношение к которым будет причиной причинения ущерба их владельцу или иному лицу.

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Смаилова Севиля Аблякимовна
магистрант
Таврическая академия ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ЭЛЕКТРОННАЯ ПОДПИСЬ

Информация на сегодняшний день один из основных ресурсов, потеря которого может привести к неизбежным последствиям. Чтобы предотвратить данную ситуацию используют всевозможные методы защиты информации.

Любой программист или же специалист в области информационных систем изучает целый комплекс форм и способов безопасности информационных сетей. Тем не менее, человек, работающий с секретной информацией должен знать виды информационных угроз и способы

защиты от потери данных. Несанкционированный доступ преступников к каким-либо данным, является одним из главных видов информационных угроз.

Применение современных методов, предотвращающих потерю информации, являются основой технологии защиты информации. Цель каждого способа защиты - это создание действенной технологии защиты данных, при которой потери из-за невнимательности исключены. Для защиты информационных систем, которые предназначены для передачи по сети используют методы шифрования и защиты электронных документов.

Одним из таких является электронная подпись – аналог обычной подписи, которая имеет юридическое значение. Используется для процедуры обмена защищенными данными через интернет.

Существует четыре типа электронных подписей.

1. Простая. Используется в рамках предоставления государственных услуг, фактически это логин и пароль.
2. Неквалифицированная. Создается с помощью специальных программных средств. Данная подпись позволяет определить лицо, подписавшее документ, и защитить его от несанкционированного изменения.
3. Квалифицированная. Отличается от неквалифицированной электронной подписи тем, что выдается аккредитованным удостоверяющим центром.
4. Универсальная. Карта, которая может хранить, как и сертификат электронной подписи, так и личные данные, и платежную функциональность.

Электронную подпись можно использовать в любой географической точке страны, следовательно, она является доступной для всех. Для того чтобы оградить себя от электронного мошенничества нужно всего лишь обезопасить токен, изменить первоначальный пароль. Необходимо заметить, что токен не подлежит взлому, а так же восстановлению пароля.

В данный момент электронный обмен документов и как следствие электронные подписи стали активно распространяться по стране. Постепенно электронные данные замещают бумажные. Однако есть моменты, которые замедляют этот процесс:

1. Неграмотность большинства населения в использовании компьютера;
2. Отсутствие в документах прямого действия указаний на повсеместное применение электронной ответственности;
3. Слабая защита информации.

Бумажные документы, которые заверены подписью ответственного лица и печатью организации, имеют ту же юридическую силу, что и электронные документы, заверенные электронной подписью. Таким образом, имеющаяся система обмена электронными документами, заверенными электронной подписью, в целом решила главную проблему электронного обмена документами: приравняла электронные документы с электронной подписью к документам на бумажных носителях, оформленных соответствующим образом.

УДК 330.46

Кинторяк Екатерина Николаевна
старший преподаватель кафедры бизнес-информатики
АНО «ООВО» «Университет экономики и управления»
Республика Крым, Россия, e-mail: Lena.KEN@mail.ru

ОБ АСПЕКТАХ ИССЛЕДОВАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И ВОПРОСАХ ЕЁ ЗАЩИТЫ

Постановка проблемы. Интеллектуальная собственность является движущей силой производственных процессов экономической системы РФ. Пополнение резервов интеллектуальной сферы общества зависит от степени сохранности и защищённости интеллектуальной собственности. **Актуальность** работы заключается в необходимости изучения проблем, связанных с исследованием специфики интеллектуальной собственности, как наиболее перспективной части интеллектуального потенциала Российской экономики. **Целью исследования** является исследование сущности интеллектуальной собственности и её защиты.

Анализ исследований и публикаций. Проблемой исследования интеллектуальной собственности занимались широко известные российские учёные: Л. С. Шаховская, Б.Б. Леонтьев, В. Л. Иноземцев, А. Н. Козырев, Е. А. Ленская, а также зарубежные учёные: В. М. Порохня, Г. Беккер, Е. Бруклинг, Б. Вейсброда, Т. Бьюзен, Д. Даффи, Д. Клейн, Л. Эдвисон, Д.

Снайдер, М. Мелоун, Г. Минс, Т. Шульц, Б. Л. Хансен, российские учёные: Л. С. Шаховская, Б.Б. Леонтьев, В. Л. Иноземцев, Е. А. Ленская.

Многочисленные исследования отечественных и зарубежных авторов обосновывают зависимость прогрессивного продвижения общества от уровня развития его интеллектуального ресурса. Это особенно актуально в период перехода от индустриальной к постиндустриальной стадии развития, когда возрастает роль знания и информации. Актуальной темой становится их охрана. На фоне данного процесса происходит усиление значения интеллектуальной собственности, которое все более определяет ее социальные приоритеты и жизненные перспективы. Известный экономист Козырев А. Н. даёт многоплановое понимание нематериальных активов предприятия. В табл. 1 помещены различные трактовки понятия нематериальных активов применимо к разным областям экономической деятельности.

Таблица 1.

Понятие нематериальных активов в различных сферах экономической деятельности

№	Сферы экономики	Понятие НА
1	Бухгалтерское понимание НА	*Идентифицируемые НА*: интеллектуальная собственность и некоторые другие имущественные права, способные приносить доход более одного года;
2	Понятие НА в оценочной деятельности	*Неидентифицируемые НА*: капитализированные расходы на создание юридического лица. Все НА, как учитываемые на балансе, так и не учитываемые (персональный гудвилл и совокупная обученная рабочая сила).
3	Понятие НМА в налоговом законодательстве	приобретенные и (или) созданные налогоплательщиком результаты интеллектуальной деятельности и иные объекты интеллектуальной собственности (исключительные права на них), используемые в производстве продукции (выполнении работ, оказании услуг) или для управленческих нужд организации в течение длительного времени (продолжительностью свыше 12 месяцев).
4	Налогообложение	Способность приносить налогоплательщику экономические выгоды (доход); наличие надлежаще оформленных документов, подтверждающих существование самого нематериального актива; исключительного права у налогоплательщика на результаты интеллектуальной деятельности (патенты, свидетельства, другие охранные документы, договор уступки (приобретения) патента, товарного знака).

Личные качества персонала организации (интеллектуальные и деловые), квалификация и способность к труду к нематериальным активам не относятся. Нематериальные активы выделяют, как результат интеллектуальной деятельности. Организация имеет права на результат интеллектуальной деятельности. Способность приносить организации экономические выгоды (доход) в будущем и использование в производстве продукции, при выполнении работ или оказании услуг либо для управленческих нужд организации – основные характеристики нематериальных активов. Существует возможность идентификации НА организацией от другого имущества, не предполагается последующая перепродажа данного актива; первоначальная стоимость НА может быть достоверно определена. НА в широком смысле: достижения науки, литературные труды, произведения искусства; программы для ЭВМ и других компьютерных устройств; программы для ЭВМ, базы данных с целью нахождения и их обработки; изобретения, полезные модели; селекционные достижения, секреты производства («ноухау»), товарные знаки и знаки обслуживания; деловая репутация фирмы (гудвилл). Права на обладание нематериальными активами являются их юридическим содержанием, их можно отнести к особому виду НА: исключительное право патентообладателя на изобретение, промышленный образец, полезную модель; на использование программы для ЭВМ, базы данных; топологии интегральных микросхем; на товарный знак, знак обслуживания, наименование места происхождения товаров и фирменное наименование; на селекционные достижения; на владение ноу-хау, секретной формулой или процессом. Особой формой НА является ноу-хау (знания, не отчуждаемые от конкретного человека или от предприятия, которые могут повышать стоимость предприятия, но не могут быть активами). Деловая репутация юридического лица и goodwill также принадлежат к НА, она не передается от одного работника к другому, но влияет на распределение прибыли между сотрудниками. Разность между ценой сделки и материальными активами предприятия оформляли как особый актив и заносили на баланс покупателя, поэтому

название – добрая воля (goodwill) подчеркивало добрую волю покупателя заплатить за что-то известное обеим сторонам, но пока не отраженное на бумаге. Также к НА относятся товарные знаки и репутации. Товарный знак идентифицирует продукт или услугу коммерческого предприятия. Товарный знак является символом деловой репутации, символизирует гудвилл бизнеса. Брэнд, как вид нематериальных активов – это коммерческое воплощение репутации, формирующее стратегию маркетинга и репутацию предприятия. Уникальность бренда состоит в том, что под одним семейством товарных знаков могли бы предлагаться несколько брэндов и наоборот, бренд считается деловым эсперанто. Есть существенное отличие бренда от продукта: продукт – это то, что изготовлено для продажи, в то время как брэнд – это то, что клиент покупает. Любая собственность нуждается в охране. Интеллектуальная не является исключением. Однако способы охраны права на объекты интеллектуальной собственности специфичны. Материальный объект собственности достаточно поместить под «замок» или приставить к нему сторожа, то для охраны объектов интеллектуальной собственности такие средства непригодны. Основным способом охраны в этом случае является выдача автору или другому субъекту права объекта интеллектуальной собственности охранительного документа: патента или свидетельства. Суть охраны прав на объекты интеллектуальной собственности заключается в том, что автор объекта интеллектуальной собственности или другое признанное законом лицо получает от государства исключительные права на созданный объект интеллектуальной собственности на определенный период времени. Эти права регламентируются специальным охранительным документом.

Часто охрану интеллектуальной собственности отождествляют с ее защитой и пользуются термином «защита прав интеллектуальной собственности». Необходимо различать эти два понятия на том основании, что, во-первых, охрана и защита интеллектуальной собственности имеют разные цели, а во-вторых, осуществляются разными организационными структурами. Охраной (оформлением прав с выдачей охранительного документа) занимаются патентные органы, а защитой (в случае нарушения этих прав) - административные и судебные органы. Для роста благосостояния различных слоев общества каждая страна нуждается в развитой и хорошо налаженной системе интеллектуальной собственности. Охрана интеллектуальной собственности способствует сохранению национального потенциала в сфере интеллектуальной деятельности, привлечению инвестиций, стабилизации экономического положения государства, при котором отечественные и иностранные инвесторы могут быть уверены, что их права интеллектуальной собственности соблюдаются. Необходимым элементом зрелой государственности является наличие в государстве современной международной системы охраны интеллектуальной собственности. Создание такой системы имеет особое значение для России - государства со значительным научно-техническим интеллектуальным потенциалом.

Таким образом, в настоящее время успех и развитие современного производства в конкурентной среде все в большей степени зависит от интеллектуальной собственности, уровня её защищённости и качественной охраны. В компаниях, организациях все в большей степени доминируют не основные фонды и материальные запасы, а информация, знания и другие элементы интеллектуального капитала.

УДК 338 : 004.772

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Бутенко Татьяна Владимировна
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

«Облачные технологии» это технологии обработки и передачи данных, при применении которых доступ пользовательским данным и приложениям, их обрабатывающим, осуществляется через сеть Интернет.

Сейчас во всем мире происходит бурное развитие «облачных технологий» и прогнозируется постепенный перевод существующих информационных систем в «облако».

Предлагаются к использованию различные типы «облачных» сервисов – публичные, частные и гибридные. Для облегчения перехода провайдеров услуг и потребителей на облачные

технологии необходима стандартизация переносимости данных, оценки качества сервисов, защиты данных приложений и пользователей, принятие государственными органами соответствующих нормативно-правовых актов и стандартов.

«Облачные технологии» применяются различными пользователями для разнообразных задач.

Разработкой стандартов в сфере «облачных вычислений» занимается множество международных и региональных организаций, таких, как Open Cloud Consortium (OCC), Cloud Security Alliance (CSA), Distributed Management Task Force (DTMF), Cloud Standards Customer Councll, IEEE, National Institute of Standards and Technology (NIST), OASIS, Storage Networking Industry Association (SNIA), группа по облачным вычислениям в составе Open Group, европейская ETSI и другие.

В России вопросы принятия стандартов, норм и правил в области информационной безопасности, возложены на Федеральную службу по техническому и экспортному контролю - ФСТЭК.

К сожалению, до сих пор не приняты изменения в Закон РФ 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», которыми бы вводились понятия «облачных сервисов», «провайдера облачных услуг» и т.п. на законодательном уровне, что способствовало бы развитию «облачных» услуг в Российской Федерации. Сейчас идет обсуждение и доработка проекта изменений в данный Закон.

Несмотря на наличие пробелов в законодательстве, провайдеры «облачных» услуг, действующие в России, проводят добровольную сертификацию своих сервисов и систем на соответствие международным стандартам ISO, европейским стандартам ETSI, стандартам США NIST, отраслевым стандартам и рекомендациям.

В странах Европы и США провайдеры облачных услуг почти всегда сертифицированы по рекомендациям ISO 27001:2013 – системы менеджмента информационной безопасности. В России ему соответствует ГОСТ Р ИСО/МЭК 27001-2006, основанный на более ранней версии этого стандарта от 2006 года.

Наличие у провайдера облачных сервисов сертификатов соответствия рекомендациям ISO 20017 и ISO 20001 в области информационной безопасности негласно признается достаточным для обеспечения уровня безопасности предоставляемых услуг. Но особенность применения этих рекомендаций заключается в том, что выполнять их необходимо не только провайдеру, но и его клиентам, например, в реализации правил контроля доступа у клиента к своей информации в «облаке». Новшеством является взаимная ответственность провайдера «облачного» сервиса и его клиента за безопасность информации.

Для ведения бухгалтерского учета, как правило, применяются «облачные» сервисы SaaS – программное обеспечение, как услуга. Клиент оплачивает доступ к услугам провайдера «облачных» услуг, куда входит аренда программного обеспечения, антивирусная защита, техническая поддержка пользователей сервиса, обновление программ согласно изменениям в законодательстве, создание резервных копий и т.п. Для абсолютного большинства предприятий малого и среднего бизнеса, индивидуальных предпринимателей достаточно предлагаемых стандартных функций. Доступ к сервису осуществляется из сети Internet через браузер или с использованием технологии «тонкий» клиент.

Как следствие, из вышеперечисленного выводятся и относительные неудобства использования «облачных» сервисов. Требуется наличие постоянного подключения устройств пользователя к сети Internet, не всегда совместимы с предлагаемой системой некоторые версии браузеров, иногда требуется обучение клиентов дополнительным навыкам работы с программным обеспечением, при прекращении договора с провайдером данные клиента могут быть удалены безвозвратно.

Преимуществ использования облачных сервисов гораздо больше. Это отсутствие привязки к офису, доступ к сервисам большому количеству пользователей в любое время, сокращение расходов на IT персонал, информация физически размещена в охраняемых сертифицированных датацентрах с автоматическим резервированием, проверки правоохранительных органов не приводят к остановке работы из-за изъятия компьютерной техники и многое другое.

Для крупных предприятий со множеством филиалов с развитой информационной структурой перевод бухгалтерского и управленческого учета в «облако» требует тщательной проработки процесса перехода со стороны как ИТ подразделения и высшего руководства, так и со стороны провайдера облачных услуг. Выполнение рекомендаций стандартов и провайдером и клиентом поможет правильно осуществить переход и воспользоваться всеми преимуществами «облачных» сервисов.

Планируемый перевод государственных услуг в цифровую форму и оказание их через сеть Internet даст мощный импульс развитию «облачных технологий» в РФ. Появляется мощный потребитель и разработчик «облачных сервисов» – государство. Ускорится разработка и утверждение необходимых стандартов, норм и правил, необходимых при применении облачных сервисов.

Сегодня многие специалисты в области экономики и финансов прогнозируют стремительное развитие рынка «облачных» сервисов.

Приняты многие российские ГОСТы и стандарты, соответствующие международным стандартам и правилам в области «облачных вычислений» и сервисов.

Проводится общественное обсуждение проекта поправок в Закон РФ 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», в котором вводится понятие «облачных сервисов».

Внедрение и переход к «облачным технологиям» обязывают провайдеров услуг и их клиентов совместно выполнять требования существующих и внедряемых стандартов информационной безопасности при использовании «облачных технологий».

УДК 338.001

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Губарева Дарья Александровна
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ОСНОВАННЫХ НА НЕЧЕТКОЙ ЛОГИКЕ

Сегодня обеспечение безопасности персональных данных является одной из острейших проблем в информационной сфере и взаимоотношениях государства, юридических и физических лиц. К примеру, логистические компании оперируют большими потоками разнородных данных, которые должны оставаться конфиденциальными. Поэтому транспортные предприятия, совершенствуя свои технологии, ставят перед собой цель не только в увеличении оперативности и точности операций, но и в способности защитить данные в их программном обеспечении. Интеллектуальные информационные системы являются качественно новым подходом в решении транспортных задач, при этом, многие системы безопасности строятся на основе искусственного интеллекта, в том числе, на основе нейронных сетей.

Поскольку субъекты в транспортной технике и планировании не могут быть отделены от процессов восприятия и принятия решений человеком, транспортные задачи являются хорошей областью для применения теории нечеткой логики. На самом деле, уже было сделано значительное число попыток применить теорию нечетких множеств к проблемам транспорта.

Теория нечетких множеств облегчает моделирование ситуаций, которые описываются как приблизительные или туманные. Чаще всего, нечеткое множество представляет собой концепцию, связанную с естественным языком. Таким образом, эта теория полезна при анализе качественных или описательных данных и моделирования системы, свойства которой описаны или выражены только на естественном языке.

Классическая транспортная задача может быть обобщена в модифицированной транспортной задаче, включая в себя сразу три параметра - поставок, спроса и перевозочных мощностей. Если перед экспертом-логистом стоит цель найти значения более чем одного параметра, то задача называется многоцелевой модифицированной транспортной задачей (ММТЗ). Х. Дж. Циммерман был первым исследователем, который ввел нечеткий подход программирования для обработки нескольких целевых проблем и создал нейронную сеть, основанную на нечеткой логике.

Нечеткие нейронные сети (НС) основываются на нечетких множествах и нечеткой логике (функция принадлежности элемента к множеству, принимает любые значения в интервале [0,1]. Эти НС отличаются тем, что для их элементов нет однозначного ответа относительного какого-либо свойства, поэтому необходимо использование характеристической функции (функции принадлежности), которая указывает на степень принадлежности каждого члена пространства рассуждения к данному нечёткому множеству. Таким образом, нечеткие нейронные сети

применяются тогда, когда необходимо использование недостаточно формализованных или лингвистических переменных.

Метод гибридных нейронных сетей также использует аппарат нечеткой логики, но функция принадлежности в нем способна обучаться и подстраиваться. Гибридная нейронная сеть напоминает по строению многослойную нейронную сеть с обучением, но скрытые слои в ней соответствуют этапам функционирования нечеткой системы. Такие системы не только используют поступившую от пользователя информацию, но и могут получать новые знания, используя различные методы обучения. Данные нейронные сети целесообразно использовать для задач, в которых нет четкого деления элементов на классы. Также гибридные нейросети применяются для задач, зависимости в которых не линейны и задач, в которых необходимо рассмотрение влияния большого количества разных факторов. Гибридные сети очень функциональны и могут решать большое количество экономических задач, но наряду с этим, они являются сложными в использовании. Из-за отсутствия формализованных алгоритмов настройки нейронной сети, требуется специальная подготовка пользователей, так как существует необходимость самостоятельно задавать форму и размеры нечетких множеств.

ММТЗ была решена несколькими исследователями с использованием различных методов. И. Ли и К. Ида вскоре представили генетический алгоритм для решения ММТЗ с коэффициентами целевой функции в виде нечетких чисел. Кроме того, ими был разработан подход нейронной сети для многокритериальной ТЗ, а также улучшенный генетический алгоритм для решения ММТЗ с нечеткими числами. А. Чарнс и В.Купер впервые описали подход целевого программирования (ЦП). Целевое программирование - это причудливое название, описывающее очень простую идею: грань между целями и ограничениями нельзя определить однозначно. В частности, когда существует целый ряд задач, то, как правило, лучше определить некоторые из них или все в качестве ограничений, а не отдельно взятых целей.

Постановка задачи решения ММТЗ на основе нечетких методов целевого программирования состоит из 4 шагов и приведена ниже:

Шаг 1. Решить проблему многокритериальности путем выделения каждый раз только одной цели (r=1,2,…,R) при этом игнорируя все остальные для получения оптимального решения $X^{r*} = x_{ijk}$ из R для каждого отдельного параметра.

Шаг 2. Вычислить значения всех целевых функций R для всех R оптимальных решений $X^{r*}(\mathbf{r = 1, 2, \dots, R})$ и найти нижнюю и верхнюю границы для каждой целевой функции, заданной $L_t = \dot{Z}_t(X^{t*}), t = 1,2, \dots R$ и $U_t = Max\{\dot{Z}_t(X^{1*}), \dot{Z}_t(X^{2*}), \dots \dot{Z}_t(X^{R})\}$.

Шаг 3. Определить функцию принадлежности μ_t целевой функции R следующим образом:

$$\mu_t(\dot{Z}_t(x)) = \begin{cases} 1, \text{если } \dot{Z}_t \le L_t \\ \dfrac{U_t - \dot{Z}_t}{U_t - L_t}, \text{если } L_t \le \dot{Z}_t(x) \le U_t \\ 0, \text{если } \dot{Z}_t \ge L_t \end{cases}$$

Шаг 4. Решить полученную модель, используя заданные параметры, полученное решение будет наиболее эффективным для ММТЗ.

Разработка методов решения логистических задач – это хорошо развитое направление в интеллектуальном анализе данных. Благодаря появлению таких методов существует возможность как решить задачи, стоящие перед экспертом, так и защитить данные от внешнего вмешательства. Это стало возможно благодаря усовершенствованию программного обеспечения по созданию нейронных сетей, решения задач с помощью генетических алгоритмов, а также целевого программирования.

Основная проблема всех систем, функционирующих на основе искусственного интеллекта в том, что они требуют огромное количество качественных данных, без которых обучение не будет продуктивным. Соответственно, собирая в облаке или на диске информацию, компания рискует её потерей. Но при этом, хорошо налаженная интеллектуальная система в разы упрощает работу по обеспечению мер средств защиты информации и генерирует новые, оптимальные, возможно даже не столь очевидные человеку.

УДК 004.056.52 : 336.7

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Панченко Игорь Александрович
магистрант
ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И ВЫБОР НАИЛУЧШЕЙ МОДЕЛИ ДЛЯ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Развитие общества и информатизации привело человечество к пониманию того, что каждый из нас живет в информационном обществе, которое в свою очередь представляет не только технологическую базу но и организацию системы взаимоотношений между производителями, потребителями и доступом к информации.

Информационное общество стало создаваться с появлением первого компьютера, появления первых сетевых технологий, Интернета.

На каждом этапе, библиотечная система внедряла все больше новых технологий стараясь идти в ногу со временем, развивая, внедряя и совершенствуя доступ к накопленным знаниям и ресурсам. Сегодня библиотечная система является неотъемлемой частью культурного наследия нашей страны, а так же главным хранителем знаний и ценностей Российского государства.

В эпоху развития информационных технологий все большее число библиотек стараются сохранить свое место в информатизации общества, обеспечив пользователей необходимой и доступной информацией, внедряя новейшие технологии для предоставления максимального количества услуг и необходимого доступа к информации для потребителей.

На современном этапе библиотечных технологий наиболее перспективными и популярными являются «облачные» технологии, потому что позволяют обеспечить максимальный спектр услуг в любое время и в любом месте. В свою очередь, многие библиотечные системы склоняются к внедрению именно «облачных» технологий учитывая их качество, стоимость и степень защищенности. Но все ли так хорошо?

Помимо основных типов угроз, таких как угрозы которым подвержено программное обеспечение, сетевые угрозы и прочие, облачные технологии подвержены так же специфическим угрозам безопасности.

Рассмотрим основные модели «облачных» технологий и угрозы безопасности присущие каждой из них:

1. Инфраструктура как сервис. (IaaS);

Эта модель представляет собой систему, в которой покупатель пользуется приложениями продавца услуг. Как правило, в таких моделях используют интерфейс браузера или приложение, разработанное продавцом услуг.

У этой модели существуют следующие угрозы безопасности, которые необходимо учитывать при выборе, а именно:

- совместный доступ пользователей к оборудованию «облака». При атаке, или изъятии другого пользователя «облачной» системы, могут пострадать и другие участники «облака»;
- защищенность интернет каналов. Вся работа в облачной системе напрямую связана с использованием интернет каналов, что в свою очередь требует надлежащей защиты и правильной аутентификации, использования шифрования и мониторинга работы сетей;
- DoS атаки наверное, самый большой недостаток «облачных» технологий. При подобных атаках, клиенту приходиться платить поставщику за использованный трафик, который по сути не был получен;
- распределение доступа к ресурсам между клиентами «облака». Все мощности распределяются не равномерно, а по принципу «кто первый».

2. Платформа как сервис (PaaS).

Это модель, которая предоставляет покупателю доступ к использованию прикладного программного обеспечения, систем управления базами данных, операционных систем, средств тестирования и разработки программного обеспечения.

Ей присущи следующие риски безопасности:

- изменение или взлом SQL запросов. Этим угрозам в большинстве подвержены базы данных, которые использует пользователь в «облаке»;
- XSS представляет собой уязвимость, при которой имеется возможность внедрения в HTML страницу скрипта с вредоносным кодом;
- распространение вредоносных программ внутри приложений;
- атаки на интерфейс прикладного программирования. Атаки на базовые компоненты платформы;
- атаки на передаваемые данные. Перехват данных при передаче от клиента к «облаку»;
- атаки на клиента. Перехват паролей, данных учетных записей и другое.

3. Программное обеспечение как сервис (SaaS).

Эта модель включает в себя набор инструментов присущих предыдущим моделям и позволяет управлять «облачными» средствами хранения и обработки, использовать прикладное программное обеспечение, разрабатывать собственное программное обеспечение, хранить информацию, использовать и управлять базами данных.

Для этой модели наиболее характерными являются такие угрозы:

- сетевые угрозы. За счет того, что доступ к облаку осуществляется через Интернет — оно является частью общественного ресурса, который подвержен сетевым атакам, таким как: вирусные программы, подборы паролей, подмены клиентов, DDos-атаки - многочисленные и постоянные запросы сайта приводящие к затруднению доступа пользователей или отказу;
- утечки и потери информации. Потери информации из-за отказа оборудования. Потери информации вследствие действий инсайдеров, причем как со стороны «облачного» сервиса (администраторы), так и со стороны покупателей;

Хотелось бы отметить тот факт, что «облачные» технологии является еще относительно молодым информационным решением, которое будет развивать свою структуру и соответственно меры безопасности. Последние несколько лет показали экономический эффект и удобство внедрения таких технологий. Учитывая риски в информационной безопасности, внедрение «облачных» технологий в библиотечную систему России окажет значительный экономический эффект, обеспечит удобство пользователям и сотрудникам библиотечной системы.

Из вышеуказанного становится ясно, что полностью безопасных «облачных» систем не существует, но поставщики услуг постоянно совершенствуют технологии защиты своих клиентов. Главным аспектом при достижении максимальной безопасности, наверное, стоит выделить поставщика услуг и правильный его выбор. Ведь безопасность выбранной модели в большей степени зависит от него. Говоря о самих моделях облачных услуг можно сказать, что IaaS модель менее остальных подвержена воздействию угроз, но предоставляет наименьший спектр возможностей для потребителя. Модели PaaS и SaaS больше подвержены воздействию угроз безопасности, но позволяют в полном объеме обеспечить необходимые возможности для пользователя.

УДК 32.019

Курунов Александр Владимирович,
доцент, к.т.н.
Ткаченко Сергей Павлович,
доцент, к.т.н.
ФГБОУ ВО «Самарский государственный университет путей сообщения»
Россия

СИСТЕМА АВТОМАТИЗИРОВАННОГО АДМИНИСТРИРОВАНИЯ И ПРОВЕРОК БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕРВИСОВ

В современных условиях высокого уровня угрозы в отношении государственных учреждений по стороны киберпреступников на первый план выходит проблема безопасности информационных сервисов ВУЗа. Известно, что в образовательных учреждениях всегда остро проявляется проблема нехватки высококвалифицированных специалистов по системному администрированию и информационной безопасности. Это связано с тем, что из-за неадекватного соотношения квалификации и финансового стимулирования сотрудников образовательных учреждений мы наблюдаем довольно высокую текучесть кадров в сфере IT-технологий.

Проблемы снижения уровня информационной безопасности (аварийные остановки сервисов антивирусной защиты и фареволов) и доступности публичных сервисов (электронная почта, WEB-сервер, сервер дистанционного обучения) особенно критичны во время, когда оперативное сопровождение работающих сервисов поручается «молодому специалисту».

С целью минимизации таких угроз в Самарском государственном университете путей сообщения (СамГУПС) используется методология IT Infrastructure Library — библиотеки инфраструктуры информационных технологий (1С-ITIL) и база знаний по инцидентам. Хотя это и облегчает обучение, но не избавляет от ошибок администрирования, что и приводит к высокому времени реакции на угрозы со стороны обслуживающего персонала. На наш взгляд, одним из способов решений этой проблемы является внедрение автоматизированного администрирования критичных ресурсов IT-инфраструктуры. Решение данной задачи облегчается тем фактом, что работа системного администратора включает в себя часто выполняемые типовые задачи задачи. Но рекомендуемый в литературе подход к автоматизации при помощи написания и выполнения в нужный момент скриптов, опять же требует работы администратора высокой квалификации, т.к. персоналу приходится анализировать критичную ситуацию и принимать решения в условиях острого дефицита времени.

Очевидно, что большинство организаций использует те или иные системы мониторинга сети, которые доступным языком умеют самостоятельно оповещать о проблемах посредством электронной почты. После получения почты, сотруднику необходимо достаточно большое время чтобы осознать проблему, найти решение и подключиться к нужному серверу с консоли или по удаленному доступу.

Например, в случае зависания SQL сервера, в лучшем случае уходит около 30 секунд чтобы прочесть почтовые сообщение о сбое, около минуты чтобы соединиться по RDP, и около 30 секунд чтобы открыть панель управления и перезапустить сервис, то есть порядка 2 минут. Поэтому актуальным является создание инструмента ИТ-специалиста, совмещающего в себе средства информирования о проблемах в инфраструктуре, поддержки принятия решений и контроля их исполнения. Инструмент для обеспечения безопасности и доступности сетевых сервисов должен повышать скорость реагирования дежурного системного администратора на возникающие угрозы. Именно в возможности поручить работу менее квалифицированному сотруднику, который выполнит её за приемлемое время, заключается основная цель автоматизации. Следовательно, для выполнения вышеперечисленных условий инструмент автоматизации администрирования должен иметь интуитивно-понятный интерфейс с широким уровнем использованием естественных языков и разработанными скриптами на основе типовых ситуаций.

В СамГУПС реализован один из подходов к созданию такого инструмента, в виде чат-робота (бота) для мессенджера Telegram, структура которого показана на рис. 1.

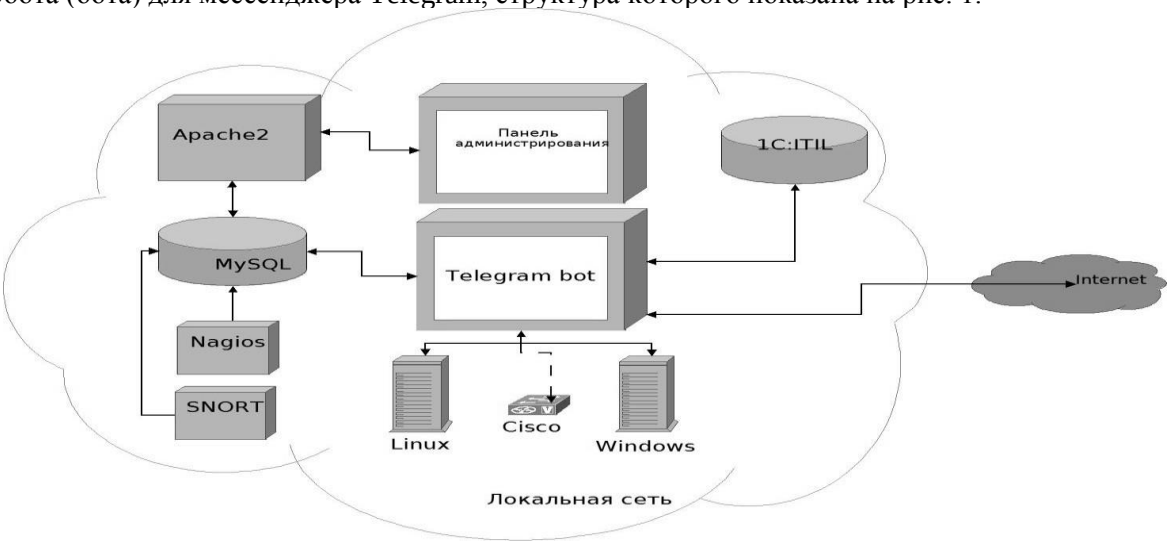


Рис. 1. Структура бота

Код написан на языке Python с применением библиотеки telebot и выполняется в несколько потоков. В одном потоке происходит обработка действий пользователя, в остальных — запрос данных от внешних систем мониторинга (Nagios, SNORT, 1С:ITIL) и выдача сообщений от них. Приходящие от систем мониторинга сообщения рассылаются по определенным группам, за исключением сообщений от 1С:ITIL, которые приходят только пользователям указанным в

маршруте документа 1С. Для Linux систем скрипты автоматизации выполняются посредством ssh, для Windows систем используется psExe.

Структура меню и другие данные бота хранятся в базе данных MySQL. Связь с 1С реализована посредством протокола SOAP.

Панель администрирования бота реализована на языке php в виде веб-приложения, позволяющего редактировать настройки бота, которые хранятся в таблицах MySQL. Это приложение позволяет редактировать структуру меню бота, определять выполняемые команды, создавать пользователей, группы пользователей, определять права доступа к командам меню, различные настройки. Как для разных групп пользователей можно задать индивидуальный набор меню, так и для каждого вида информационного сообщения так же можно задать состав меню, отображаемый вместе с сообщением.

Пользователю, не прошедшему авторизацию доступна только команда /Login, при помощи которой он привязывает свой идентификатор чата Telegram к аккаунту системы. При успешной авторизации аккаунта ему становятся доступны команды системного администрирования. С целью последующего контроля и разбора ошибок каждое действие пользователя записывается в журнал активности.

Безопасность в случае утери смартфона с установленным чат-ботом обеспечивается правилами безопасности ОС Android (заблокированный загрузчик, обязательный пин-код для разблокировки, выключенная отладка adb), а так же возможностью оперативно заблокировать пользователя из панели администрирования.

Поскольку при использовании бота перезагрузка SQL сервера занимает около 30 секунд, то работа администратора в данном случае ускоряется в 4 раза. Таким образом, данная система позволит повысить оперативность и безопасность системного администрирования работающих сервисов.

УДК 004.055

Пенькова Инесса Вячеславовна
д.э.н., профессор
Асанов Сервин
магистрант
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ

Конфиденциальная информация представляет повышенный интерес для конкурирующих предприятий. Некоторые проблемы зачастую связаны с недостаточной оценкой важности угрозы, по причине чего предприятие терпит крах либо в конечном итоге становится банкротом. Источниками таких угроз в основном являются конкуренты.

Особую ценность для конкурентов представляет ознакомление с защищаемой информацией, а также ее максимальное искажение в целях причинения ущерба, к чему может привести даже 15-ти процентная утечка информации, что может произойти в результате неопытности сотрудников или вследствие отсутствия систем защиты. Данные и информация, находящиеся в собственности компании, подвержены определенным угрозам.

1) Угрозы конфиденциальности программного обеспечения и информации, возникающие после несанкционированного доступа к информационных ресурсам.

2) Угроза доступности. Такая ситуация не позволяет нужному пользователю применять службы и ресурсы, что происходит по причине их захвата, получения по ним информации или блокировки линий кибер-злоумышленниками. В результате искажается достоверность, адекватность и своевременность транслируемой информации.

3) Внутренние угрозы, источником которых становятся неопытность, некомпетентность или низкая квалификация персонала.

Для разработки адекватной защиты информации учитываются всевозможные варианты угроз, и варианты их возникновения. Обеспечение информационной защищенности предприятия реализуется таким образом, чтобы злоумышленник столкнулся с множеством проблем на всех этапах уровней защиты. К наиболее эффективному методу защиты ПО и информации относится алгоритм с крипто-шифрованием при пересылке данных, когда система зашифровывает не только доступ, но и саму информацию, что актуально и для безопасности информации всех сфер

деятельности. Структура доступа к информации должна быть многоуровневой, в связи с этим, к ней разрешается допускать лишь определенных сотрудников. Право полного доступа ко всему объему информации должны иметь только доверенные лица. В настоящее время разработаны специальные программные продукты, которые круглосуточно следят за любыми изменениями и состоянием сети. Чтобы избежать случайных потерь данных должны проводиться соответствующие тренинги. Это позволит предприятию контролировать готовность персонала к работе и даст руководителям уверенность в том, что все работники готовы соблюдать и обеспечивать информационную безопасность.

Реалии рыночной экономики и интенсификация конкуренции принуждают руководителей компаний и предприятий перманентно проводить мониторинг среды и мобильно реагировать на ее изменения, например, активное проникновение информационных технологий во все сферы прогресса, социально-экономические процессы развития управления функционированием бизнеса. При этом виртуальные угрозы информационной безопасности компаний могут нанести значительный ущерб, и наоборот, - обеспечение повышенной информационной защищенности становится одним из обязательных условий успеха и получения прибыли.

УДК 004.055

Пенькова Инесса Вячеславовна
д.э.н., профессор
Иванников Игорь Александрович
магистрант
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНЫХ ДАННЫХ НА FACEBOOK

Проблематика информационной безопасности личный данных в соцсетях остается актуальной и привлекает внимание исследователей. Это объясняется тем, что количество пользователей соцсетей перманентно и быстро растет, открывая новые возможности общения, при этом аккаунты пользователей взламываются, нередко бывают случаи утечки информации, а также важным фактором является наличие доступа к любой информации администрации сети. Одна существует гораздо больше потенциальных угроз для личных данных хранящихся в памяти социальных сетей.

С одной стороны, социальная сеть обещает и гарантирует полную защиту персональных данных, однако, с другой, - существуют многообразные варианты использования сетью личных данных, что приводит к их потере или краже.

Система Facebook использует личные данные без разрешения пользователя для подбора потенциальных друзей и знакомых или показа рекламы, или контента, соответствующих интересам пользователя. Такие механизмы стандартны для многих социальных сетей, что предполагает сбор и анализ персональных данных, предоставляемых пользователем в необходимом объеме, и дальнейшее их использование в коммерческих целях. После чего сети передают личные данные за границы сети, что было признано официально сетью Facebook.

Также одной из важных проблем, создающих дискомфорт пользователям является утечка личных данных по вине социальной сети.

По мнению специалистов, наиболее серьезной угрозой является открытый доступ ко всем пунктам личной информации, принадлежащий большой группе людей, которые могут просматривать ее в любое время суток, не обращая внимания на то, что информация была удалена пользователем из сети.

К таким группам относятся:

во-первых, сотрудники самой сети FB так, как у них имеется доступ ко всем базам данных, которые хранят информацию обо всех пользователях, и они имеют специализированные инструменты для входа в личные аккаунты, к примеру, специальный пароль администратора;

во-вторых, представители правоохранительных органов (ЦРУ, ФСБ), что вполне закономерно, поскольку сотрудники сети не могут ограничиваться в доступе, т.к. это – их работа, и они обязаны следить за порядком и устранять нарушения, а сотрудники правоохранительных органов при помощи социальных сетей разыскивают злоумышленников. Однако это совершенно не освобождает от возможности передачи данных пользователя третьим

лицам, такими данными могут является важные конфиденциальные данные или даже психологические портреты юзеров.

В последнее время пользователи начинают меньше доверять таким социальным сетям как Facebook и больше стараются фильтровать информацию, которую считают необходимым доверить сети, либо дают ложную информацию о себе и не раскрывают свою личность, или применяя кардинальные инструменты - удаление из сети или деактивация аккаунта. Тем не менее, даже удаление из сети не может полностью гарантировать защиту, поскольку информация после удаления сохраняется на сервере компании и, в случае необходимости, может быть найдена и использована.

УДК 004.055

Пенькова Инесса Вячеславовна
д.э.н., профессор
Нурлыгаянов Осман Альбертович
бакалавр
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ЗАЩИТЫ ЛИЧНЫХ ДАННЫХ НА FACEBOOK

Несмотря на то, что Facebook предоставляет качественную защиту данных для своих пользователей, никто не застрахован полностью. Facebook является привлекательным для взлома мошенниками ресурсом.

В последнее время злоумышленники часто используют для кражи персональных данных фишинговые атаки, что дословно переводится с английского как «рыбачить». В случае компьютерного фишинга доверчивые пользователи являются «пойманной рыбой», а для того, чтобы ее поймать, мошенники используют поддельные e-mail-сообщения или создают практически безошибочные копии наиболее популярных веб-сайтов, в том числе и Facebook.

Составляя фишинговое письмо, хакеры стараются максимально приблизить его к стилю и оформлению официальной рассылки от Facebook. Текст этого сообщения обычно содержит руководство к действию, чтобы «выудить» информацию, например, это может быть предложение восстановить пароль в целях безопасности. Встроенная в сообщение ссылка отправляет пользователя на сайт злоумышленников - точную копию Facebook. Авторизовавшись на фиктивной странице, пользователь вводит свои логин и пароль и отправляет их непосредственно недоброжелателям.

Отметим, что существуют многообразные разновидности фишинговых атак, и не все они относятся к Facebook. Неоднократно киберпреступники отправляли подобные письма от имени известных банков или крупных онлайн-магазинов, чтобы незаконно завладеть данными банковских карт клиентов. Одним общим фактором у фишинговых атак является то, что мошенники всегда стремятся выбрать представительные и надежные компании с широким кругом клиентов.

На практике применяются различные методы для защиты от фишинга. Но в основе любого из них лежат внимательность и осторожность, в первую очередь, самого пользователя, особенно в те моменты, когда в сообщении предлагают ввести личные данные в онлайн-режиме.

Есть несколько правил, соблюдение которых обезопасит пользование Facebook и поможет избежать хакеров:

1) Не рекомендуется вводить личные данные в ответ на e-mail-запрос.
2) В случаях, если ссылка в формате HTML, находящаяся в сообщении, выглядит точной копией страницы Facebook, персональную информацию следует вводить только при условии безопасного соединения, когда в строке URL web-сайта, его адрес будет начинается с «https://» и в интерфейсе браузера появится иконка замка.
3) Все входящие e-mail требуют проверки на наличие репрезентативных признаков подделки: орфографических ошибок и наличие слов, побуждающих срочно отправить данные. Если в письме указана ссылка, отличающаяся от адреса сайта Facebook, то это является признаком фишинговой атаки.
4) Не целесообразно переходить по ссылкам в письмах, чтобы избежать мошенников. Следует открыть нужный веб-сайт в новом окне, скопировав или введя адрес вручную.

5) Браузер, антивирус и другое ПО должны содержать свежие – до последней версии – обновления безопасности.

6) Письма, которые вызывают подозрения, необходимо отправлять в техподдержку социальной сети для уведомления о возможной попытке взлома.

Таким образом, повышение уровня безопасности личных данных участников сети Facebook обеспечивается лично пользователем с учетом предлагаемых непосредственно соцсетью возможностей.

УДК 004.58

Семенова Юлия Андреевна
старший преподаватель
Институт экономики и управления (структурное подразделение)
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СРЕДСТВА ЗАЩИТЫ АККАУНТА В СОЦИАЛЬНЫХ СЕТЯХ

Поскольку в современных условиях интенсификации он-лайн общения актуализируется проблематика защиты персональных данных пользователей соцсетей, то целесообразно рассмотреть ряд рекомендаций, при соблюдении которых возможность потери информации в личных аккаунтах значительно снижается.

1. Сокращение объема представляемых персональных данных в сетях.

При расположении информации на свою страницу пользователь должен осознавать, что любая размещенная информация может быть использована в чужих интересах всеми, кому открыты эти сведения. При заполнении своего профиля, необходимо выкладывать минимальную информацию.

2. Усложнение регистрационных данных.

Мошенники часто проводят взлом учетных записей с помощью сервиса «Восстановление пароля». Использование двухфакторной авторизации на сайте помогает улучшить качество безопасности страницы, для этого при входе в систему рекомендуется вводить наряду с логином и паролем, дополнительный код.

3. Провокации незнакомых людей.

Хакеры пользуются методом социальной инженерии, при помощи которых получают персональные данные, путем создания психологической ситуации, заставляя человека самостоятельно предоставлять сведения о себе.

4. Закрытие доступа к личной информации незнакомцам.

При добавлении в друзья в социальной сети других пользователей рекомендуется выбирать только знакомых в реальной жизни, поскольку злоумышленники могут скрываться под видом ребенка, девушки или парня, которые якобы просто желают познакомится. Также, в социальных сетях есть функция, которая позволяет создать несколько категорий «друзей», чтобы разграничить уровни доступа к предоставляемой информации и персональным данным.

5. Не синхронизировать контакты.

Если синхронизировать социальную сеть с контактным данными телефона и электронного ящика будут использованы не только ваши данные, но и данные людей, занесенных в ваши контакты.

6. Переход только по надежным ссылкам.

Не целесообразно переходить в свой аккаунт по ссылкам из спамных электронных сообщений или с различных сайтов, поскольку злоумышленники давно используют множество фейк-страниц.

7. Отключение вручную ненужных сервисов.

С развитием инновационных IT-технологий для персональных данных появилась еще одна угроза – геосоциальные сервисы, оповещающие посторонних о местоположении пользователя на карте: Facebook Places, Google Lattitude, Foursquare и др. Если пользователь использует сеть в офисе, то появляется возможность заражения рабочего компьютера или корпоративной сети в целом. По умолчанию в социальные сети включена опция автораспознавания лиц, которую необходимо отключать в ручную. В социальной сети общим средством безопасности при входе и пребывании там является использование защищенного протокола взаимодействия с Web-серверами https, гарантирующего безопасную передачу данных по сети, хотя и снижающего скорость передачи.

Тем не менее, сложно полностью обезопасить от нападения личный аккаунт. Наиболее легким и надежным способом максимально защитить персональные данные при активном пользовании соцсетей является уменьшение объема предоставляемой личной информации и настройка опций и функций аккаунта вручную для освобождения от ненужных дополнительных сервисов, собирающих информацию о пользователе.

УДК 681.142.2

Сергиенко Елена Николаевна
канд. физ.-мат. наук, доцент
Вожакова Юлия Викторовна
студент
Белоусова Наталья Владимировна
студент
Институт энергетики, информационных технологий и управляющих систем
ФГБУ ВО «БГТУ имени В.Г.Шухова»
Белгород, Россия

МЕТОДЫ ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Специалисты в области информатики, программирования, криптографии, защиты информации постоянно сталкиваются с необходимостью работы со случайными числами и последовательностями случайных чисел. Генераторы случайных чисел используют алгоритмы, которые заранее определены, детерминированные алгоритмы. Из этого следует, что полученные последовательности являются псевдослучайными, так как рано или поздно любой генератор начинает повторять последовательность чисел и является периодическим.

Решением этой проблемы может быть генерация псевдослучайной последовательности с достаточно большим периодом, чтобы конечная последовательность не была периодической и соответствовала статистическим критериям на случайность, например, критерию χ^2 (хи - квадрат). Данный критерий позволяет оценить вероятность того, что данная выборка является выборкой значений случайной величины с заданным законом распределения.

Для применения критерия χ^2 с помощью наблюдаемого значения χ_0^2 и значения степеней свободы v по таблице распределения χ^2 (рис. 1) необходимо найти вероятность (*P*) истинности гипотезы о том, что исследуемая выборка подчинена равномерному закону распределения, так как эталонная псевдослучайная последовательность подчинена именно этому закону.

	$p = 1\%$	$p = 5\%$	$p = 25\%$	$p = 50\%$	$p = 75\%$	$p = 95\%$	$p = 99\%$
$\nu = 1$	0.00016	0.00393	0.1015	0.4549	1.323	3.841	6.635
$\nu = 2$	0.02010	0.1026	0.5754	1.386	2.773	5.991	9.210

Рис. 1. Некоторые процентные точки χ^2 – распределения

Если *P* слишком мало или слишком велико, то генератор не удовлетворяет требованию равномерного распределения. «Хорошим» является значение *P* от 25% до 50%, приемлемым от 10% до 90%.

Наиболее распространенными алгоритмами генерации псевдослучайных последовательностей являются линейный конгруэнтный метод и метод Фибоначчи с запаздыванием.

Кроме этих стандартных методов применяется метод генерации псевдослучайных двоичных последовательностей на основе клеточных автоматов. К основным достоинствам этого метода относятся контролируемый период и хорошие статистические свойства псевдослучайных последовательностей, эффективность и высокое быстродействие аппаратной реализации генераторов.

Клеточный автомат – дискретная модель, включающая регулярную решётку ячеек $y[i]$ любой размерности, каждая из которых может находиться в одном из конечного множества состояний, например таких как 1 и 0. Для работы клеточного автомата требуется задание начального состояния всех ячеек и правил перехода ячеек из одного состояния в другое. На каждой итерации, используя правила перехода и состояния соседних ячеек, определяется новое состояние каждой ячейки. Поскольку граничные ячейки решетки обладают меньшим количеством «соседей», то они отличаются от других ячеек, что противоречит свойству однородности. Для решения этой проблемы противоположные края n-мерной решетки

отождествляются, что для одномерных клеточных автоматов равносильно «скручиванию» решетки в кольцо, а для двумерных — в тор.

В программной реализации генерации псевдослучайных двоичных последовательностей используется одномерный клеточный автомат, представленный в виде цепочки из 9 клеток. Пусть функция состояний клетки имеет следующий вид:

$\mathbf{y'[i] = y[i-1]}\ xor\ (y[i]\ or\ y[i+1])$, где $\mathbf{y'[i]}$-новое значение выбранной клетки, $y\mathbf{[i]}$-выбранная исходная клетка, $y\mathbf{[i-1]}$ - клетка перед $y\mathbf{[i]}$, $y\mathbf{[i+1]}$ - клетка после $y\mathbf{[i]}$.

Описанными методами были программно получены псевдослучайные последовательности длины 150. Выполненный статистический анализ полученных псевдослучайных последовательностей согласно критерию χ^2 выявил следующие результаты. Для последовательности, полученной методом клеточного автомата, χ^2=0,1067 и 25%< P <50%, что соответствует «хорошему» значению P. Для последовательности, полученной при помощи линейного конгруэнтного метода, χ^2=0,06 и 1%< P <5%, что слишком близко к теоретическим значениям и не может рассматриваться как случайная последовательность. При методе Фибоначчи с запаздыванием последовательность имеет χ^2=6 и 75%< P <95%, что показывает значительную удаленность получаемых значений от теоретических и может быть приемлемым для псевдослучайной последовательности, но не «хорошим».

УДК 34:004

Тутова Ольга Васильевна
канд.педагог.н.,
кафедра гуманитарных
и социально-экономических дисциплин,
Крымский филиал Краснодарского университета МВД России
Республика Крым, Россия

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И МЕТОДЫ ИХ РАССЛЕДОВАНИЯ

Широкое распространение информационно-коммуникационных технологий и внедрение персональных компьютеров во все сферы жизни современного общества привели к возникновению нового вида преступлений, которые связаны с информационными технологиями. Данное явление представляет собой специфический и достаточно новый вид преступного посягательства.

Согласно толковому словарю компьютерные преступления – это противоправные действия, при которых персональный компьютер является либо объектом, против которого совершается преступление, либо инструментом, который используется для совершения преступных действий. Немного иной смысл содержится в более кратком определении данного понятия из юридического и экономического научно-технического словаря, в котором определяется, что компьютерные преступления – это преступления в сфере компьютерной информатики.

С юридической точки зрения такое определение рассматриваемого понятия уравнивает блокирование компьютерной системы Министерства обороны с целью подрыва обороноспособности страны, незаконное копирование или распространение авторского программного продукта, кража принтера или убийство путем нанесения удара украденным ноутбуком, например, по голове потерпевшего.

В.Б. Вехов определяет компьютерные преступления как предусмотренные уголовным законодательством общественно опасные деяния, в которых объектом преступного посягательства является информация в электронном виде. В данном случае в качестве предмета или орудия преступления будет выступать информация в электронном виде, компьютер, компьютерная система или компьютерная сеть.

В.С. Комиссаров утверждает, что преступления в сфере компьютерной информации – это умышленные общественно опасные деяния, которые причиняют вред или создают угрозу причинения вреда общественным отношениям, регламентирующим безопасное создание, обработку, хранение, использование и распространение информации и информационных ресурсов либо их защиту.

Следовательно, компьютерные преступления – это преступления, которые представляют собой любое незаконное или неразрешенное поведение, затрагивающее хранение, передачу данных или автоматизированную обработку данных. Следует отметить, что компьютерная информация в данном случае является предметом или средством совершения преступления.

Анализируя уголовные дела по преступлениям, которые были совершены с использованием средств компьютерной техники, можно выделить свыше 40 их основных

разновидностей. Причем число разновидностей компьютерных преступлений постоянно увеличивается в связи с использованием преступниками различных комбинаций и логических модификаций этих алгоритмов.

Рассмотрим наиболее распространенные преступления в сфере информационно-коммуникационных технологий и действия, которые необходимо выполнить сотруднику правоохранительных органов в процессе их расследования.

Если преступление связано с несанкционированном доступом к компьютерной информации, то в ходе расследования сотруднику правоохранительных органов необходимо осуществить такие действия:

1) установить факт неправомерного доступа к информации в электронном виде в компьютерной системе или сети;

2) установить место и время несанкционированного проникновения в компьютерную систему или сеть (как правило, на практике определить место и время непосредственного применения технических средств удаленного несанкционированного доступа очень сложно);

3) установить надежность средств защиты компьютерной информации;

4) установить способ несанкционированного доступа (чаще всего с помощью специальной информационно-технической судебной экспертизы);

5) установить лица, которыми был совершен неправомерный доступ, и мотив преступления. Анализ следственной практики показывает, что чем сложнее способ совершения преступления в техническом отношении, тем проще найти подозреваемого, так как круг специалистов, обладающих соответствующими техническими способностями, обычно ограничен;

6) выявить обстоятельства, способствовавшие совершению преступления и установить вредные последствия случившегося.

Такая схема действий сотрудника правоохранительных органов при расследовании преступлений в сфере информационно-коммуникационных технологий является актуальной и наработанной годами.

При расследовании преступлений, связанных с созданием, использованием и распространением вредоносных программ используется такая последовательность действий.

1. Установить факт и способ создания вредоносной программы.
2. Установить факт использования и распространения вредоносных программ.
3. Установить личности, виновные в создании, использовании и распространении вредоносных программ для персональных компьютеров.
4. Установить вред, причиненный данным преступлением.
5. Установить обстоятельства, способствовавшие совершению расследуемого преступления.

При расследовании преступлений, связанных с нарушением правил эксплуатации персональных компьютеров или компьютерной сети, необходимо доказать факт нарушения определенных правил, который повлек за собой уничтожение, модификацию или блокирование компьютерной информации, охраняемой законом, и размер нанесенного ущерба. Кроме этого, необходимо установить и доказать следующие факты:

1) место и время (период времени) нарушения правил эксплуатации персонального компьютера или компьютерной сети;

2) характер компьютерной информации, подвергшейся уничтожению, модификации или блокированию вследствие нарушения правил эксплуатации компьютерной системы или сети;

3) способ и механизм нарушения правил эксплуатации персонального компьютера или компьютерной сети;

4) характер и размер ущерба, причиненного содеянным преступлением;

5) факт нарушения определенным лицом правил эксплуатации компьютера;

6) виновность лица, допустившего преступное нарушение правил эксплуатации персонального компьютера;

7) обстоятельства, способствовавшие совершению расследуемого преступления.

Таким образом, рассмотренные нами схемы деятельности сотрудников правоохранительных органов при расследовании основных типов компьютерных преступлений являются базовыми. Они могут дополняться другими пунктами, однако целью всех выполняемых действий является получение максимального количества информации о совершенном компьютерном преступлении и, как следствие, нахождение виновного в совершенном преступлении.

УДК 004.056.08

Бойченко Олег Валерьевич
д.т.н., профессор,
Бахши Д. Г.
студент 4-го курса бакалавриата заочного отделения
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Следует подчеркнуть, что в настоящее время основным механизмом защиты данных в сетях является шифрование информации.

При помощи процедуры шифрования отправитель сообщения преобразует его из простого текста в набор символов, не поддающийся прочтению без применения специального ключа, известного получателю. Получатель сообщения, используя ключ, преобразует переданный ему набор символов обратно в текст (рис. 1).

Т.о., если информация в зашифрованном виде попадет к злоумышленнику, он просто не сможет ей воспользоваться.

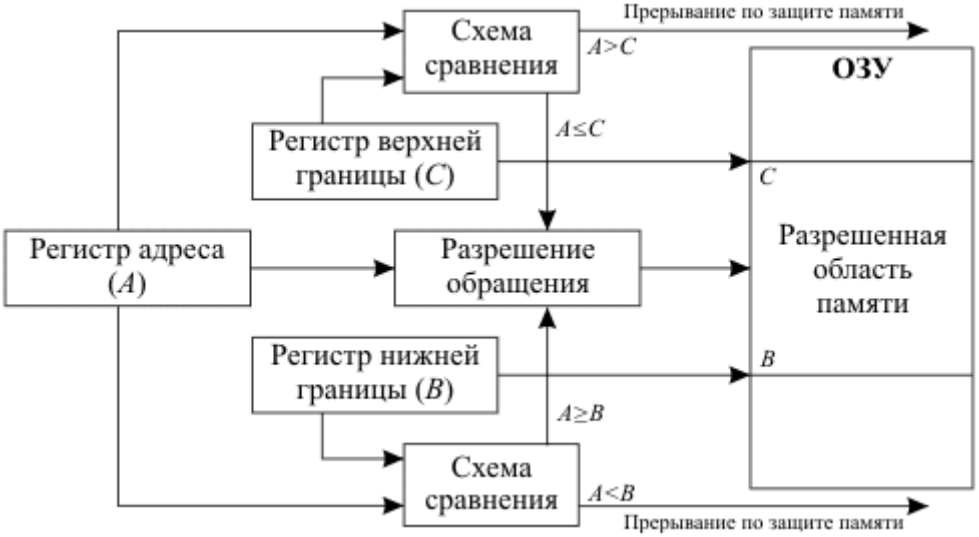


Рис. 1. Схема передачи данных с использованием процедуры шифрования

Авторизационный сервер (authentication server), обрабатывает все запросы пользователей на предмет получения того или иного вида сетевых услуг, получая запрос от пользователя, обращается к БД и определяет, имеет ли пользователь право на совершение данной операции.

Пароли пользователей по сети не передаются, что также повышает степень защиты информации.

Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера «пропуск», содержащий имя пользователя и его сетевой адрес, время запроса и ряд др. параметров, уникальный сессионный ключ. Пакет, содержащий «пропуск», передается также в зашифрованном виде.

После получения и расшифровки «пропуска» сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем дает «добро» на использование сетевой аппаратуры или программ.

Особо следует подчеркнуть, что протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

Идеально подходит для применения в Интернет и аналогичных сетях.

Основная концепция состоит в том, чтобы определить, если есть секрет, известный только двоим, то любой из его хранителей может с лёгкостью удостовериться, что имеет дело со своим напарником. Для этого ему достаточно проверить, знает ли его собеседник общий секрет.

Простой протокол аутентификации с секретным ключом вступает в действие, когда кто-то стучится в сетевую дверь и просит впустить его.

Чтобы доказать своё право на вход, пользователь предъявляет аутентификатор (authenticator) в виде набора данных, зашифрованных секретным ключом.

Получив аутентификатор, привратник расшифровывает его и проверяет получен информацию, чтобы убедиться в успешности дешифрования. Содержание набора данных должно постоянно меняться, иначе злоумышленник может просто перехватить пакет и воспользоваться его содержимым для входа в систему.

Если проверка прошла успешно, то это значит, что посетителю известен секретный код, а так как этот код знает только он и привратник, следовательно, пришелец на самом деле тот, за кого себя выдаёт.

Три участника безопасной связи: клиент, сервер и доверенный посредник между ними. Роль посредника здесь играет так называемый центр распределения ключей Key Distribution Center (KDC), представляющий службу, работающую на физически защищённом сервере.

Она ведёт БД с информацией об учётных записях всех главных абонентов безопасности своей области. Вместе с информацией о любом абоненте безопасности в БД KDC сохраняется криптографический ключ, известный только этому абоненту и службе KDC. Этот ключ, который называют долговременным, используется для связи пользователя системы безопасности с центром распределения ключей.

В большинстве практических реализаций протокола Kerberos долговременные ключи генерируются на основе пароля пользователя, указываемого при входе в систему. Когда клиенту нужно обратиться к серверу, он, прежде всего, направляет запрос в центр KDC.

В ответ на запрос клиента, который намерен подключиться к серверу, служба KDC направляет обе копии сеансового ключа клиенту.

Сообщение, предназначенное клиенту, шифруется посредством долговременного ключа, общего для данного клиента и KDC, а сеансовый ключ для сервера вместе с информацией о клиенте вкладывается в блок данных, получивший название сеансового мандата (session ticket).

Затем сеансовый мандат целиком шифруется с помощью долговременного ключа, который знают только служба KDC и данный сервер.

Вся ответственность за обработку мандата, несущего в себе шифрованный сеансовый ключ, возлагается на клиента, который должен доставить его на сервер.

УДК 004.77

Журавленко Николай Иванович
к.ю.н., доцент
Олюшкевич Олег Витальевич
бакалавр
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

В современном мире постоянно происходит борьба за информацию. Очень часто возможно появление третьего лица, заинтересованного в использовании коммерчески ценной информации, например – в её продаже. Именно поэтому для безопасной передачи данных потребуется не только оборудование, которое её осуществляет, но также и специальные алгоритмы, благодаря которым информация может быть скрыта от посторонних. Таким образом для обеспечения безопасности передачи данных потребуется две составляющие: аппаратная и программная. Под аппаратной частью подразумевается специализированное оборудование, обеспечивающее передачу данных, а под программной частью понимаются программные средства обработки этих данных.

Беспроводная сенсорная сеть – это система беспроводных датчиков и исполнительных устройств, связанных между собой по радиоканалу. Узел беспроводной сенсорной сети состоит из мотов - устройств, снабженных различными сенсорами (температуры, геолокации и др.) и передающим устройством, которое передаёт информацию в заданном диапазоне частот по радиоканалу. Мот представляет собой простое устройство, состоящее из процессора, оперативной и флэш памяти, цифро-аналогового и аналого-цифрового преобразователя, радиочастотного приемопередатчика, подключенных к нему датчиков, а также элементов питания. Простота данного устройства объясняется отсутствием необходимости хранения большого количества данных и выполнения сложных арифметических операций, что позволяет

снизить и его энергозатраты. Всю информацию, в конечном счете, моты пересылают специальному устройству – шлюзу. Шлюз имеет соединение с корпоративной сетью, которое может быть организовано проводным соединением с сетью Интернет, или беспроводным соединением посредством мобильной сети GPRS или радиоканала Wi-Fi.

Сенсорные сети получили своё распространение относительно недавно. Начиная с 2000 года благодаря развитию микроэлектроники появилась возможность на основе таких систем строить очень дешевую элементную базу, что привело к широкому развитию систем данного класса. По своей сути, сенсорные системы позволяют объединить окружающую среду с цифровым миром. Поэтому существует очень много сфер и мест применения данных систем. Например, широким спросом эти системы могут пользоваться в сферах промышленности, транспорта, сельского хозяйства, метеорологии, охраны.

Так как данная статья посвящена вопросам обеспечения безопасности, рассмотрим применение сенсорных систем в отрасли охраны. Для осуществления охраны какого-нибудь объекта можно построить целую сеть сенсоров, таких как датчики движения, света, температуры и т.д. Причем эти сенсоры могут быть установлены в самых уязвимых и труднодоступных местах охраняемого объекта. Собирая информацию со всей сенсорной сети, можно иметь полное представление о состоянии безопасности объекта, причем этот способ охраны позволит оптимизировать количество сотрудников службы охраны, улучшить степень безопасности, исключить человеческий фактор при принятии решений и уменьшить вероятность допущения ошибки.

Поскольку данная система работает в сфере безопасности и вся собираемая с неё информация имеет высокую ценность, то особую актуальность приобретает задача обеспечения защиты самой сенсорной системы и собранной с ее помощью информации от действий злоумышленников. Если эти данные будут передаваться в открытом виде, то злоумышленник их может перехватить, найти уязвимость в системе, или, что ещё хуже, подменить их. Это нарушит статус безопасности объекта и сделает его подверженным угрозам. Поэтому чрезвычайно важно в этой системе обеспечить безопасную передачу данных, которая, в свою очередь, обеспечит также их целостность.

Способы атаки на беспроводные сети схожи со способами атак на проводные сети. При этом беспроводные сети защитить сложнее, поскольку они не имеют изолированной среды для передачи данных, а это означает, что получить доступ к ним проще. Для этого может использоваться шифрование и специальная система аутентификации сенсоров.

В качестве средств шифрования могут быть использованы различные алгоритмы, начиная с простых TEA и XTEA, и заканчивая более сложными, например, AES. Проблема выбора применяемых алгоритмов шифрования находится в прямой связи с уровнем энергопотребления устройства, что для систем данного класса критически важно. Поэтому в системах данного класса более рационально использовать простые алгоритмы либо ассиметричного шифрования с открытым ключом, либо симметричного шифрования. При этом потребуется использование специальной системы аутентификации для того, чтобы злоумышленник не мог загрузить систему, отправляя ложные сообщения. Для этого уже существуют готовые решения, основанные на стандарте IEE802.15.4, определяющем физический слой для беспроводных сетей с маломощными приемо-передатчиками. Например, спецификация ZigBee, которая имеет высокую степень безопасности благодаря использованию симметричного ключа. Но при этом следует заметить, что никаких стандартов в области используемого программного обеспечения пока не существует. Именно поэтому в системах данного класса могут использоваться различные протоколы передачи и обработки данных, в которые внедряют протоколы безопасности, разработанные под конкретную структуру и задачи данной беспроводной сети.

Беспроводные сенсорные сети являются активно развивающимися, они уже нашли свое применение в агрессивных, безопасно-зависимых средах, что делает их подверженными различным угрозам. Поэтому обеспечение безопасности таких сетей является приоритетной задачей. В данной статье были рассмотрены общие вопросы обеспечения безопасности в сенсорных сетях, возможности их использования в системах охраны, а также механизмы их защиты от различных угроз.

УДК 004.77

Журавленко Николай Иванович
к.ю.н., доцент
Скиба Мария Михайловна
бакалавр
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

На текущий момент времени информационные технологии составляют технический фундамент для обеспечения практически всех аспектов человеческой жизни. Большинство предприятий использует технологии локально-вычислительных сетей для хранения и доступа к индивидуальным и сетевым ресурсам. Значение локально-вычислительных сетей заключается в распределении ресурсов, данных, а также программных средств при объединении и систематизировании электронно-вычислительных машин в единую сеть. Вследствие этого, обеспечение состояния защищенности сети становится главным критерием ее надежности, а также показателем ее эффективности. Актуальность проблемы обеспечения сетевой безопасности состоит в масштабе наблюдаемых последствий от непосредственно угроз, а также в невозможности обеспечить тотальное отсутствие уязвимостей сети.

В общем случае, под сетевой безопасностью принято понимать совокупность требований к сетевой инфраструктуре, а также комплекс мероприятий, направленных на обеспечение защиты от сетевых атак, а также угроз несанкционированного доступа. Система, обеспечивающая информационную безопасность, должна представлять собой иерархическую структуру, состоящую из защиты автоматизированных рабочих станций, защиты локально-вычислительных сетей и серверов, а также защиты корпоративной автоматизированной системы.

Инфраструктура сети представляет собой совокупность аппаратных и программных средств, таких, как: маршрутизаторы, коммутаторы, сервера удаленного доступа, а также каналы передачи данных. Исходя из этого, обеспечение защищенности инфраструктуры достигается с помощью технических решений: изоляция внутренних сетей, блокирование или ограничение прав доступа к тем или иным аппаратным средствам или данным. К примеру, установление приоритетов сетевого трафика при передаче помогает избежать нарушения целостности информационного пакета, а также минимизировать сетевые задержки.

Среди угроз сетевой безопасности, равно как и среди угроз информационной безопасности, существуют: угрозы конфиденциальности, целостности, доступности, а также истинности или достоверности информации, полезности и управляемости. Программная реализация той или иной угрозы с помощью набора алгоритмов представляет собой сетевую атаку и в основном направлена на незащищенные протоколы, а также на уязвимости сетевой инфраструктуры. Невозможно создать условия, при которых сетевые атаки отсутствовали бы. Основным решением для обеспечения защищенности от атак является устранение обнаруженных уязвимостей вследствие исправления ошибок в программной среде, обеспечение целого ряда проверок подлинности идентификаторов, а также усиление подсистем защиты. Направленность работы по защите сетевого сервера заключается в предотвращении или налаживании нормальной работоспособности узла WEB-сервера, на который нацелена атака, защита от нарушения целостности, изменения или удаления данных, а также защита от завладения привилегированным доступом организатором атаки. К обеспечению защиты WEB-сервера относят: устранение ошибок при администрировании, к примеру, запрет на использование некоторых методов, а также усовершенствование программных решений при реализации алгоритмов самого сервера и доступа к нему, в том числе различных серверных приложений.

Вследствие этого, возникает вопрос анализа защищенности сети, а также оценки и поиска возможных уязвимостей, как основного вектора для модификации и усовершенствования системы защиты сети. В общем виде мероприятия по анализу защищенности сети включают в себя: изучение структуры автоматизированной системы, оценку риска возможных угроз безопасности в направлении данных и ресурсов системы, оценку различных уязвимостей системы, а также обеспечение или усовершенствование механизмов по обеспечению защиты. Широко применяются такие методы исследования, как: сканирование внешних сетевых адресов, активное и пассивное тестирование системы защиты и анализ серверных конфигураций. Среди методов тестирования системы существуют: тестирование без предварительного сбора данных о конфигурации тестируемой системы, а также тестирование, основанное на знаниях о структуре и

конфигурации испытуемой системы. В первом случае задействуются все известные типы атак. Для анализа испытания используются сетевые сканеры, содержащие информацию об известных уязвимостях. Во втором случае проверяются алгоритмы, конфигурация и механизмы по обеспечению безопасности системы. Оценка рисков и уязвимостей в данном случае осуществляется с помощью программных утилит, анализирующих защищенность системы. Не менее значимой в тестировании системы является система обнаружения атак, состоящая из средств сбора и анализа информации, а также средств управления и реагирования.

В связи с широким распространением виртуальных частных сетей возникает угроза несанкционированного доступа ко внутренним сетевым ресурсам при передаче по открытой сети. Также существует угроза несанкционированного доступа до внутренним данным корпоративной сети по причине несанкционированного входа в сеть злоумышленником. Следовательно, для защиты информации в открытых каналах связи, необходимо: аутентифицировать взаимодействующие стороны, подвергать данные при передаче шифрованию, а также анализировать истинность и целостность передаваемой информации. Активно используют технологию туннелирования, базирующуюся на криптозащите открытых каналов связи. Благодаря инкапсуляции пакетов в новый пакет, содержащий информацию о получателе и отправителе, осуществляется защита пакета. А цифровая подпись обеспечивает достоверность и целостность передаваемой информации.

Существуют технологии и методы, позволяющие анализировать и контролировать защищенность распределенных компьютерных системы. Одним из таких технологических решений является использование специализированного диагностического программного обеспечения. Контролируемые системы подвергаются установке специального агента, проверяющего правильность настроек и контролирующего целостность файлов. Программа-менеджер посылает инструкцию в виде команд агентам, после чего сохраняет полученные данные в базе. А программа-администратор, в свою очередь, управляет менеджерами и модифицирует политику безопасности. Использование данных программ значительно повышает надежность сети и уровень ее защищенности, однако противодействующим фактором является высокая стоимость.

УДК 004.77

Журавленко Николай Иванович
к.ю.н., доцент
Степченко Анна Владимировна
бакалавр
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Сегодня в значительной степени растёт взаимозависимость между странами, определяющаяся постоянно расширяющейся сетью Интернет. Быстрое развитие компьютеров, связанных с ними сетей и инфраструктуры толкнуло мир в «информационную эру», которая в целом распространяется на период с конца двадцатого века по настоящее время.

Информационные и коммуникационные технологии привели к распространению информации между континентами и странами мира. Именно поэтому они стали одним из столпов нынешней эпохи, привнося своим существованием множество преимуществ. В то же время, это привело к появлению новых проблем, связанных с необходимостью обеспечения информационной безопасности. С появлением Интернета и постоянно увеличивающимся количеством пользователей в нём хакеры и другие злоумышленники проводят много времени в попытке получить доступ к важной и конфиденциальной информации, которая может быть использована для материального вымогательства и морального деструктивного воздействия.

Именно поэтому критически важно заботиться о безопасности данных, передаваемых в глобальной сети Интернет, объединяющей в себе более восьми миллиардов устройств (с учётом не только персональных компьютеров, но и смартфонов, телевизоров, приставок и иных подключаемых устройств). Крайне упрощённый принцип просмотра страниц в Интернете строится на следующем: существует клиент, запрашивающий информацию, и сервер, эту информацию отдающий. То есть сервер является хранилищем данных, в которых заинтересован пользователь, являющийся клиентом. Для защиты потока данных, приходящих от клиента к серверу и уходящих в обратном направлении, применяются различные протоколы безопасности.

Они периодически совершенствуются, сменяя или модифицируя алгоритм, применяемый для шифрования трафика, как только вычислительной мощности компьютеров становится достаточно, чтобы скомпрометировать текущую версию алгоритма.

Особое внимание следует уделить безопасности самого сервера от проникновения извне. Как известно, большинство веб-приложений имеют уязвимости и могут подвергнуться атакам. Основным источником угроз для реализации уязвимостей является внешний нарушитель – лицо, имеющее коммерческий или личный интерес, обладающее знаниями и необходимой квалификацией в вопросах сетевой безопасности. Иначе внешнее лицо можно назвать хакером, а основную угрозу веб-приложения – хакерской атакой. Такая атака может носить как целевой, так и нецелевой характер. В первом случае злоумышленник может целенаправленно выявлять уязвимости в атакуемой системе, во втором же случае атака скорее является массовой с использованием известных и общих уязвимостей.

Угрозы безопасности можно разделить на три типа:

1. Угрозы конфиденциальности, то есть несанкционированный доступ к данным.
2. Угрозы целостности, то есть несанкционированное искажение или уничтожение данных.
3. Угрозы доступности, то есть ограничение или блокирование доступа к данным.

Угрозы безопасности проистекают из нескольких факторов. В первую очередь в этот список следует включить общие уязвимости и несовершенство механизмов идентификации, во-вторых, это намеренное разглашение или утечка информации о самой системе, в-третьих, это атаки на самих пользователей с целью перехвата их аутентификационных и персональных данных.

Чаще всего уязвимости веб-приложений представляют собой выполнение нежелательного кода на сервере. При обработке запроса от клиента сервер получает и анализирует переданные данные, часто они напрямую влияют на отображаемый контент, передаваясь, например, в качестве запроса в базу данных. Если не предприняты необходимые меры по обеспечению безопасности (например, не фильтруются служебные символы), то злоумышленник может легко модифицировать команды, исполняемые сервером. Примером подобной уязвимости служит SQL-инъекция.

При использовании несовершенства методов аутентификации злоумышленник может либо пытаться подменить идентификатор пользователя, либо использовать атаку на методы, которые сервер применяет для определения, имеет ли тот или иной пользователь право на конкретное действие. К подобным атакам можно отнести «брутфорс» - метод грубой силы, с помощью которого в автоматическом режиме посимвольно происходит подбор пароля пользователя, небезопасное восстановление паролей без использования двухфакторной аутентификации, фиксацию сессии.

В случае атаки на пользователей злоумышленник пользуется фактом, что между сайтом и пользователем, его просматривающим, устанавливается определённое доверие. Пользователь ожидает от приложения предсказуемого поведения и легитимного контента, и при этом не ожидает атак со стороны сайта. Типичным примером может служить XSS - атака на веб-приложение, заключающаяся во внедрении в выдаваемую им страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника.

При намеренном разглашении или утечке информации о самой системе критическими могут оказаться сведения о платформе, её компонентах и составляющих, особенно в случае, когда платформа находится в открытом доступе в виде исходного кода. Возможно так же и раскрытие информации в результате неверной настройки веб-сервера или некорректной конфигурации приложения.

Чаще всего на сайтах не используются специальные средства защиты и мониторинга или нет специалиста, занимающегося вопросом информационной безопасности. Из-за подобной халатности злоумышленникам удаётся получить несанкционированный доступ к ресурсу. С учётом распространения сообществ и ростом количества специализированных форумов всё больше людей могут узнать о техниках атак, просто выполнив один запрос в «Google». Чтение новостей об обнаружении новых уязвимостей должно входить в обязанности специалиста по информационной безопасности. При этом не следует забывать о соблюдении качества кода и тщательной настройке доступа при разработке веб-приложения, то есть периодически необходимо устанавливать обновления используемого ПО, регулярно заниматься заменой паролей, отказываться от соблюдения скомпрометированных протоколов безопасности, скрывать в ответе сервера актуальную информацию о версии ПО и соответствующих компиляторов.

УДК 004.056.5

Орлова Елена Роальдовна
д.э.н., профессор
Баличева Александра Юрьевна
магистрант
Московский физико-технический институт
(Государственный университет)
Москва, Россия

МЕТОД ВЫЯВЛЕНИЯ APT-АТАК НА ОСНОВЕ КОМЛЕКСНОГО МОНИТОРИНГА СИСТЕМ БЕЗОПАСНОСТИ

APT – целевая атака, которая представляет собой непрерывный процесс несанкционированной активности в атакуемой инфраструктуре. Такие атаки, по данным Kaspersky Lab, могут иметь длительность 100 дней и более. APT - сложный класс кибератак, который практически невозможно обнаружить. Целостность, конфиденциальность и доступность данных становится под угрозу. Ущерб, наносимый компаниям от реализации целевых атак, растет из года в год. Современные системы защиты не способны выявить целевую атаку даже на поздней стадии. Понимание, интерпретация и корреляция данных, поступающих из всех систем в инфраструктуре, является основным подходом для предотвращения и обнаружения целевых атак.

Целенаправленная атака, как правило, состоит из 4 этапов: сбор информации об атакуемой инфраструктуре, внедрение и получение доступа к инфраструктуре, компрометация критичных сервисов и узлов, похищение данных и сокрытие следов. Целенаправленные атаки могут осуществляться как для похищения данных, так и для их изменения. На каждом этапе атака может осуществляться с помощью нескольких модулей. Справиться с ней отдельными системами защиты становится все сложнее.

Пример: злоумышленники выявили работника в атакующей инфраструктуре и передали флэш-накопитель с скрытым бэкдором (программа скрытого и быстрого получения доступа к данным). Работник подключил флэш-накопитель к своей рабочей станции, ничего не подозревая, запустил бэкдор. Программа позволяет несанкционированно и удаленно управлять скомпрометированным компьютером. Злоумышленник может копировать файлы и передавать их по сети, получить доступ к реестру и вносить изменения. При этом бэкдор может быть не замечен и будет отсутствовать в списке активных приложений или процессов, может быть переименован под стандартный процесс операционной системы. Казалось бы, в этом случае стандартный антивирус мог бы выявить вредоносную программу, а средство мониторинга трафика – обнаружить передачу файлов по сети. Сигнатуры и тайм-аут активности вредоносной программы могут быть изменены, тогда антивирус может не обнаружить бэкдор. Во многих случаях необходимо реализовать комплексный подход к обнаружению и предотвращению целевых атак.

Для того, чтобы обнаруживать аномалии и события, связанные с целевыми атаками, необходимо тщательно отобрать источнии данных, событий и трафика, которые будет анализировать система защиты. Комлексный подход подразумевает под собой нормализацию данных, полученных из разных источников с дальнейшей корреляцией и выявлением инцидентов. Что касается сетевого уровня защиты, система должна охватывать данные трафика (передаваемые пакеты, адреса и порты источника и назначения, используемые протоколы, заголовки и полезную нагрузку пакетов), обнаруживать вредоносный веб-трафик (отслеживать уязвимые протоколы и порты, заголовки HTTP и URL), использовать информацию систем обнаружения и предотвращения вторжений IPS/IDS (статистика по трафику в сети, известным сетевым атакам). Так как злоумышленник рано или поздно достигает локальной инфраструктуры, может копировать и манипулировать ресурсами инфраструктуры, необходимо отслеживать трафик, проходящий через локальную сеть. Для того, чтобы контролировать изменения в реестрах конечных станций, нужно получать системные данные. Данные отладки, поведения основных программ, загрузки операционной памяти, изменения файлов. Необходимо осуществлять мониторинг процессов в ядре систем и использовать данные от IDS о переполнении буфера, изменений конфигурации, подборах паролей на конечных станциях или серверах. Получив данные с большого количества источников, система должна нормализовать их и скореллировать между собой. Ведь настоящая проблема – выявлять события, которые могут не наносить ущерба сами по себе, но могут быть частью большой целевой атаки.

Модель системы защиты от APT

Такой подход к предотвращению и обнаружению APT- атак является комплексным и всесторонним, позволяет повысить степень защищенности инфраструктуры, свести к минимуму или избежать расходов от последствий успешной реализации целевой атаки.

УДК 004.056

Плетнёв Павел Валерьевич
аспирант кафедры «Безопасность и управление в телекоммуникациях»
ФГБОУ ВО «СибГУТИ»,
тел.+7-923-655-03-00, e-mail: Pavel-Pletnev@rambler.ru
Белов Виктор Матвеевич
д.т.н., профессор,
профессор кафедры «Безопасность и управление в телекоммуникациях»
тел.+7-963-906-84-83, e-mail: vmbelov@mail.ru
ФГБОУ ВО «СибГУТИ», 630102, Новосибирск, ул. Кирова, 86

АЛГОРИТМ ОПРЕДЕЛЕНИЯ ВЕЛИЧИНЫ ПОТЕНЦИАЛЬНОГО УЩЕРБА ОТ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В качестве направления развития исследуемой методики была выбрана двухфакторная модель оценки рисков ИБ, выражающая риск ИБ как произведение вероятности реализации угрозы на потенциальный ущерб. Таким образом, на основе данных таблицы, можно сделать вывод о том, что оценка потенциального ущерба осуществляется экспертным путём либо рассчитывается как ожидаемые среднегодовые потери и является итоговым результатом оценки рисков ИБ.

Помимо ранее рассмотренных подходов, мною были изучены подходы к оценке ущерба, основанные на использовании экономической теории , а также подходы, применяемые в страховой деятельности .

На основе изученного материала было принято решение использовать модель оценки ущерба от загрязнения окружающей среды . Данная модель позволяет учесть различные виды ущерба и общий вред для системы в результате инцидента, расчёт производится по формуле 1.

$$У = (У_А + У_В + У_З) * S \quad (1)$$

где $У$ – общий экологический ущерб;
$У_А$ – ущерб от загрязнения атмосферы;
$У_В$ – ущерб от загрязнения гидросферы;
$У_З$ – ущерб от загрязнения земель;
S – оценка общего экологического состояния.

В переложении данной модели для оценки ущерба в результате происшествия инцидентов ИБ было принято решение оценивать следующие виды ущерба:

– административный (административная ответственность: взыскания, ограничения на ведение деятельности);

– репутационный (потеря клиентов, инвесторов и т.д.);

– финансовый (любые потери денежных средств).

Для каждого показателя были предложены вербальные шкалы и эквивалентные им числовые показатели в относительных единицах. В таблице 2 представлены принятые шкалы для оценки видов ущерба.

Самой неблагоприятной ситуации для каждого вида ущерба присваивается наибольший вес, наиболее благоприятной, соответственно – наименьший.

Таблица 2 – Принятые шкалы для оценивания потенциального ущерба

Административный ущерб	Отсутствует	Административные взыскания	Ограничения на ведение деятельности	
	0	1	5	
Финансовый ущерб	Отсутствует	Незначительные потери *(1-5% от прибыли за определённый период)*	Умеренные потери *(6-20% от прибыли за определённый период)*	Значительные потери *(21-50% от прибыли за определённый период)*
	0	1	3	5
Репутационный ущерб	Отсутствует	Незначительный вред	Умеренный вред	Значительный вред
	0	1	3	5

Общее состояние системы после успешной реализации угрозы было решено оценивать в зависимости от общей степени нанесённого вреда и способности продолжать ведение бизнеса. В таблице 3 представлена шкала для оценки общего состояния бизнеса.

Таблица 3 – Шкала для оценки общего состояния бизнеса

Вербальный показатель	Числовой показатель
Ведение бизнеса возможно	1
Ведение бизнеса возможно, но не в полной мере, невозможно выполнение вспомогательных функций	2
Ведение бизнеса невозможно без предварительных восстановительных работ	3

После проведения оценивания состояния бизнеса, итоговую оценку потенциального ущерба можно получить следующим образом, по формуле 2:

$$Q_{общ} = (Q_A + Q_P + Q_Ф) * S, \quad (2)$$

где $Q_{общ}$ – общий ущерб;

Q_A – административный ущерб;

Q_P – репутационный ущерб;

$Q_Ф$ – финансовый ущерб;

S – состояние бизнеса в результате успешной реализации угрозы.

Самым тяжелым последствием инцидента ИБ может стать потеря бизнеса, в таком случае, общему значению ущерба присваивается значение 50, превышающее максимально возможный результат вычислений на основе принятых показателей.

В случае, если оценку ущерба осуществляет группа экспертов, необходимо осуществить проверку согласованности экспертных мнений. Проверку такого радо можно провести путём расчёта коэффициента конкордации Кендалла, по формуле 3:

$$W = \frac{12S}{n^2(m^3 - m)}, \quad (3)$$

где S – сумма квадратов отклонений рангов каждого объекта экспертизы от средней суммы рангов;

n – число экспертов;

m – количество характеристик.

Значения рассчитываемого коэффициента лежат в диапазоне от 0 до 1, где 0 показатель абсолютной несогласованности экспертов, 1 – полной согласованности. Значения коэффициента от 0,4 до 0,6 является удовлетворительным, свыше данного диапазона – высоким.

Заключительным этапом является непосредственное определение значения риска, путём перемножения показателей величины вероятности реализации угрозы и значения потенциального ущерба. Вычисляемый результат выражен в относительных единицах. В соответствии с возможными значениями P и $Q_{общ}$ получаемые итоговые значения лежат в диапазоне от 0,01 до 50. Для облегчения восприятия была введена бинарная вербальная шкала для интерпретации значений риска:

– приемлемый риск (от 0, 01 до 8);

– неприемлемый риск (от 9 до 50).

Данные значения были определены на основе анализа методик по оценке рисков ИБ и подходов к получению и интерпретации результатов в их составе.

УДК 32.019.51

Гончарова Оксана Николаевна,
д.п.н., профессор
Спектор Софья Михайловна
магистрант
Таврическая академия
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЛАЧНЫЕ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ПОДПИСИ

Одним из востребованных направлений на современном рынке является разработка программного обеспечения для того, чтобы упростить пользовательские интерфейсы. Если этого упрощения не произойдет, то даже самая полезная технология останется в тени и не получит должного внимания.

Наглядно этот тезис можно продемонстрировать в отношении к технологии электронной Сомнений в том, что это необходимая и полезная технология нет. И на данный момент нет альтернативы для решения проблем надежной аутентификации пользователей, контроля целостности их информации и др., но, не смотря на все достоинства, электронная подпись до сих пор не внедряется массово в Интернете. В наше время борьба с клонами и не способностью отказаться от публикуемой информации в социальных сетях производится достаточно активно, но массово-примененных решений с использованием электронной подписи пока нет.

Этому есть довольно простое объяснение: технологии PKI, на которых базируется использование ЭП, являются трудными для обычного пользователя. В тоже время регулирование в отрасли предъявляет дополнительные требования к программному обеспечению, что не всегда способствует привлечению потребителя.

На ряду с этим, разработчики технологий в сфере безопасности регулярно совершенствуют свои продукты, в том числе и в сфере упрощения пользовательского интерфейса. Одним из востребованных в наши дни направлений является перенос в «облако» части криптографических преобразований, в том числе, процедур проверки и формирования электронной подписи.

Проверка электронной подписи в «облаке» − это, несомненно, шаг вперёд, имеющий много положительных сторон. Одним из таких плюсов является то, что пользователям нет необходимости устанавливать себе криптографическое программное обеспечение и следить за ходом проверки сертификатов электронной подписи. Данные действия вместо пользователей выполняет система и после проверки подписи отправляет бинарный ответ − да/нет, при этом пользователь не видит и не должен разбираться, какие технологии для этого применяются и как устроен сам процесс проверки.

Перемещение проверки подписи в «облако», относительно электронного документооборота, допускает создание публичной системы ЭДО в WWW. В данной системе существует возможность изучения документов и проверки подписей не только при непосредственной работе в «облаке», но и по интернет-ссылкам на конкретные документы. С помощью этого данная технология становится ближе и доступнее любым пользователям с помощью обычных браузеров.

Хочется отметить, что перенос технологий электронной подписи в «облако» существенно увеличивает их удобство и увеличивает интерес со стороны пользователей. Целесообразным является перенос процедуры проверки подписи в «облако» для повышения уровня безопасности информационных систем

УДК 32.019.51

Гончарова Оксана Николаевна
д.п.н., профессор
Халилова Сание Мухаметовна
магистрант
Таврическая академия
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

СОВРЕМЕННАЯ СТЕГАНОГРАФИЯ

Понятие «стеганография» в переводе означает “скрытое письмо” или “тайнопись”. Главной функцией стеганографии выступает, в отличие от криптографии не шифрование и защита информации, а непосредственно сокрытие факта передачи информации.

Криптографы нашего времени используют так называемые невидимые чернила, которые обнаруживаются лишь после специальной обработки микропленки, также часто применяют метод условного расположения символов.

Теперь же, с развитием компьютерной стеганографии возникли новые методы сокрытия информации. Любую информацию, данные можно спрятать в текстовый, звуковой, графический или видео-файл. Главным требованием выдвигается избыточность контейнера для передачи данных.

Остановимся на рассмотрении носителей информации и способах включения секретных данных в носители.

• Текст. Реализовать стеганографию для передачи секретных данных через текстовые файл можно двумя способами: 1. Задействовать регистр букв. 2. Использовать пробелы. В первом случае процесс заключается в следующем: если необходимо спрятать букву "A" в слове "stenography", то берем двоичное представление кода символа "A" - "01000001". Возьмем для обозначения бита, содержащего единицу, символ нижнего регистра, а для нуля - верхнего. Итак, после наложения маски "01000001" на текст "stenography", результат будет "sTenograAphy". Окончание "phy" не использовано, так как для сокрытия одного символа используется 8 байт, а длина строки 11 символов, таким образом последние 3 символа "лишние". Согласно данному методу, сообщение, имеющее длину N/8 символов можно спрятать в текст с длиной N.

• Графические файлы. Механизм сокрытия текста в изображении происходит по принципу замены цвета в изображении на схожий. Программа производит замену определенных пикселей, положение которых вычисляет сама. Главное отличие выбора в качестве контейнера изображения вместо текста – возможность сокрытия в графическом формате не только текстовых сообщений, но и других изображений и файлов.

• Звуковые файлы. Менее всего подозрений вызывают аудио-файлы, так как мало кто может догадаться, что музыка может содержать тайные данные. Для того, чтобы разместить информацию в формате MP3, используют избыточную информацию. При использовании других аудио-файлов появляется необходимость вносить изменения в звуковую волну, что может немного повлиять на звучание.

Таким образом, шифрование данных – направление, развивающееся с каждым днем. Существует ряд методов для передачи секретных данных, один из которых – стеганография.

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

АДДИТИВНЫЕ ТЕХНОЛОГИИ, КАК ОСНОВА ДЛЯ РАЗВИТИЯ НОВЫХ ВИДОВ МОШЕННИЧЕСТВА И УГРОЗ

В настоящее время имеется мало доказательств, чтобы сделать вывод о масштабности проблем информационной безопасности связанных с 3D-печатью, так как социальные, политические, экономические и экологические последствия ее применения еще не были широко изучены. Имеющаяся ситуация может измениться в ближайшее время, так как данная

технология развивается довольно быстро и находит свое применения даже в самых неожиданных областях.

Конечно, одним из самых больших рисков технологии 3D-печати является кража интеллектуальной собственности. Данный вопрос поднимался уже не единожды и есть все основания, чтобы говорить о том, что данная угроза, в недалеком будущем, принесет огромные убытки экономике. Ситуация усложняется слабо проработанной или вовсе отсутствующей законодательной базой.

Так, каждый 3D-принтер работает по определенному шаблону, в котором заложена информация о том, какие материалы должны использоваться в процессе печати и где их разместить. Эти инструкции представляют собой ценную интеллектуальную собственность, которая может быть украдена или изменена с целью нанесения ущерба.

Для подтверждения существенности данной проблемы, специалисты в области киберзащиты Университета имени Давида Бен-Гуриона в Негеве при участии специалистов из Университета Южной Алабамы и Сингапурского университета технологий и дизайна разработали способ взлома 3D-оборудования, который позволяет удаленно вносить изменения в печатаемые детали или влиять на процесс печати непосредственно в процессе работы принтера. Изменения практически незаметны, но впоследствии приводят к разрушению самой детали уже в процессе ее эксплуатации.

В ходе атаки исследователи получили доступ к файлам моделей деталей пропеллера дрона, которые затем производились на 3D-принтере. И всего через две минуты полета квадрокоптер начал стремительно падать с большой высоты в результате запланированного разрушения лопастей пропеллера. Вследствие падения, дрон получил множество повреждений.

Если рассмотреть данный эксперимент с глобальной точки зрения, конкретно ориентируясь на производство если не самих автомобилей и самолетов, то хотя бы некоторых их составных частей посредством аддитивных технологий, то следует отметить серьезность и масштабность данной угрозы, так как последствия атаки отсрочены во времени.

Новость о печати оружия на основе аддитивных технологий – давно не нова, но ее последствия очень важны. Так, недавно в Daily Mail продемонстрировали риск безопасности, создаваемый с помощью 3D-печатного оружия. Его сотрудники создали пистолет, который способен стрелять пулями 0.38 калибра, и команда репортеров сделала это лишь с помощью шаблонов, доступных в Интернете. Процесс печати занял 36 часов. Как только репортеры создали оружие, они переправили его поездом, при этом, без проблем прошли строгий контроль на вокзале и перевезли оружие в час пик из Лондона в Париж рядом с сотнями ничего не подозревающих пассажиров. Пусть, это был всего лишь эксперимент, но его результаты являются очень весомыми при постоянно нарастающей в мире угрозе терроризма, и заставляет задуматься о способах предотвращения подобных ситуаций.

Кроме того, появляются новые материалы, которые по прочности не уступают металлу и на основе которых может создаваться холодное оружие, такое как ножи и прочее.

Этот сценарий показывает опасность на международном уровне, так как такие виды оружия, все части которого состоят из пластика или иного материала, не могут быть обнаружены при помощи металлоискателя, а разделение целого оружия на составные части затруднит их выявление даже при частном осмотре и рентгеновском снимке.

3D-печать представляет собой отличную технологию для фальсификации. Как оказалось, это не так сложно воспроизвести какой-либо объект и экспортировать его под видом подлинного, неважно, если это предмет мебели или военная установка.

Продукция, напечатанная незаконно, поднимает серьезные вопросы безопасности, но наиболее реалистичной является гипотеза, об их использовании в акте саботажа.

Данная гипотеза относится не к далекому будущему, а к реальности нашего времени, так как многие предприятия переходят на изготовление продуктов посредством 3D-печати и вполне возможно, что файл 3D-проекта попадет в руки злоумышленников или преступников, специализирующихся на контрафакции. Эти злоумышленники могли бы начать массовое производство контрафактной продукции, или, в случае операции диверсии, производить определенные компоненты, чтобы проникнуть в цепи поставок.

Частные фирмы и государственные организации работают над способами предотвращения такого рода угрозы, однако единственного решения в настоящее время не существует. Например, корпорация Квантовых Материалов в Техасе недавно объявила о лицензировании технологии под названием «квантовые точки», которая может защитить от подделок

Фармакология – отрасль, в которой аддитивные технологии открывают новые перспективы, но, в ту же очередь, и новые опасности. Так, не затрагивая тему печати

наркотических и психотропных препаратов с преступными целями, что, несомненно, составляет угрозу, обратим внимание на создание препаратов и веществ, смертельные дозы которых мизерно малы (например, Рицин) и которые могут использоваться с целью массовых терактов.

Пусть за данной возможностью стоят годы научных исследований и чрезвычайно важных открытий для человечества, однако, данная угроза имеет место быть.

Некоторые эксперты считают, что 3D-печать - технология, которая может быстро развиваться, обеспечивая большую пользу обществу. В то же время, опираясь на все вышесказанное, можно сделать вывод, что вместе с развитием технологии растут и возможные угрозы. Поворотным моментом, в данной ситуации является доступность данной технологии по разумной цене. Следовательно, для оптимального использования аддитивных технологий и во избежание проблем в будущем необходимо своевременное предотвращение любой незаконной деятельности, основой которой является 3D-печать.

Мы проанализировали небольшую часть опасностей, которые могут быть спровоцированы развитием аддитивных технологий, однако некоторые отрасли, безусловно, нуждаются в данной инновации. Так, 3D-печать может быть использована в биомедицинской области, что открывает огромные перспективы для всей медицины и человечества в целом.

Подводя итог, следует отметить, что 3D-технология - это реальность, и она находится в непрерывной эволюции. Многие отрасли начинают принимать ее из-за ряда преимуществ, так как 3D-принтеры – это идеальное решение для малого и среднего производства при оптимальном управлении материалами и значительном снижении отходов.

УДК 338 : 004.772

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

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В РАМКАХ ПРОИЗВОДСТВА НА ОСНОВЕ АДДИТИВНЫХ ТЕХНОЛОГИЙ

Технология аддитивного производства предполагает воссоздание объектов 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 особо остро встает, когда появляется угроза нарушения не только авторских прав на частные модели конструкций, а прежде всего при угрозе интеллектуальной собственности предприятий.

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. 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.

На практике привлечение к ответственности за нарушение прав интеллектуальной собственности дело обстоит легче с авторским правом, нежели с патентным. В отличие от авторского права, патентная защита не присваивается автоматически после разработки объекта. Изобретателю нужно подать заявку на регистрацию патента в государственные органы и доказать свое право на его получение. К тому же патентная защита имеет временный характер - в среднем действует от 5 до 25 лет. И, по истечению патента, его трудно получить заново, т.к. уровень техники меняется, и скорее всего за период в 5-25 лет появятся аналоги разработки, что воспрепятствует продлению патента.

В цифровой плоскости, регулирование вопросов интеллектуальной собственности еще более усложняется. На практике была разработана система, которая в зарубежных странах поддерживается на законном уровне. В США действует Закон об Авторском Праве в Цифровую Эпоху (Digital Millennium Copyright Act от 1998года), а на территории ЕС - Директива 2001/29/ЕС Европейского парламента и Совета Европейского Союза «О гармонизации некоторых аспектов авторских и смежных прав в информационном обществе» (от 2001 года). В рамках этих законопроектов предусматривается, что сайты-хостинги выступают в роли посредников между пользователями и правообладателями. Таким образом, правообладатель может отправить администраторам сайта, на котором был размещен им принадлежащий файл (права на него) запрос с требованием удаления или запрета доступа к файлу.

В мировой практике еще не достаточно случаев описывающих нарушения прав интеллектуальной собственности предприятий связанных с производством на основе 3D-печати. 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. Данные средства защиты информации и необходимость их использования стали одними из наиболее спорных вопросов цифрового века. Как правило, средства DRM встраиваются в мультимедиа-контент или непосредственно в устройства для воспроизведения мультимедиа, где выполняют проверку на лицензионность загружаемых данных и права доступа, в случае негативного ответа, блокируют доступ к ним.

Но, большинство видов DRM защиты не являются эффективными и не выполняют свою задачу - защиту, так ккак существует множество средств для обхода ограничений по использованию файлов, включающих, не только стационарное и web-ПО, но и кибер-пиратство посредством пользовательских форумов и открытых файлообменников. Можно предположить, что средства DRM защиты будут иметь примерно тот же эффект в технологиях 3D-печати, что и с мультимедиа – будут охватывать незначительную часть ресурсов и будет множество «обходных путей» для доступа к данным.

Можно сделать вывод, 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.

УДК 336

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

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ В УПРАВЛЕНИИ СТРАХОВЫМИ РИСКАМИ

Деятельность страховых организаций зависит от множества факторов, поведение которых не всегда можно предсказать с большой вероятностью точности. Определение таких факторов возможно только при наличии определенной информации. От ее своевременности и адекватности зависит эффективность принятия управленческих решений.

Для оценки состояния информационных процессов и эффективности использования информации в страховых компаниях используют рискоориентированное управление.

Риски, возникающие в страховых организациях можно разделить на две составляющие:

–риски, связанные со страховой деятельностью (принимаемые по договорам страхования, или при обслуживании договоров);

–риски, не связанные со страховой деятельностью (природные, политические, экономические).

Но могут возникнуть и риски, связанные с отсутствием, или неточностью информации. Такое явление можно охарактеризовать как риск адекватности информации. Под этим риском понимается комплексное понятие, включающее в себя риски количества качества, своевременности, безопасности, полезности, актуальности, достоверности.

Поэтому можем констатировать, что одной из причин возникновения финансовых рисков в страховых компаниях, является наличие рисков адекватности информации.

Таким образом, управление рисками адекватности информации является одной из составляющих общей системы управления рисками, которая включает в себя всесторонний анализ совокупности имеющихся рисков, их определение, оценку и выработку механизмов контроля.

УДК 004.056.5

***Мокрицкий Вадим Андреевич*,**
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Симферополь, Республика Крым, Россия

К ВОПРОСУ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация является важнейшей составляющей в производстве и управлении разными процессами. Информационные сервисы часто подвергаются рискам, таким как, утечка любого вида информации, продолжительные перебои доступа в Интернет, хищение данных, что приводит к значительным воздействием на непрерывность бизнеса. В связи с этим возникает необходимость оценки рисков нарушения информационной безопасности. Риски требуется не только оценивать, но и уметь управлять ими.

Риск представляет собой комбинацию последствий, вытекающих из нежелательного события и вероятности возникновения события. Оценка риска количественно или качественно характеризует риски и дает возможность руководителям назначать для них приоритеты в соответствии с осознаваемой ими серьезностью или другими установленными критериями.

Согласно ГОСТ Р ИСО/МЭК 27005-2010 деятельность по оценке рисков ИБ включает следующие составляющие:

- анализ рисков информационной безопасности, в свою очередь подразделяемый на идентификацию и количественную оценку рисков информационной безопасности;
- оценивание рисков информационной безопасности.

Процесс оценки рисков информационной безопасности выглядит таким образом:

- анализ рисков информационной безопасности.
  - идентификация рисков информационной безопасности.
    - идентификация активов.
    - идентификация угроз информационной безопасности.

- идентификация существующих средств управления рисками информационной безопасности.
- идентификация уязвимостей.
- идентификация последствий.

-количественная оценка рисков информационной безопасности.

- оценка последствий.
- оценка вероятностей.
- определение уровня (величины) рисков информационной безопасности.

- оценивание рисков информационной безопасности.

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

Оценка риска часто проводится за две (или более) итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, служащих основанием для дальнейшей оценки. Следующая итерация может включать дальнейшее углубленное рассмотрение потенциально высоких рисков. В тех случаях, когда полученная информация недостаточна для оценки риска, проводится более детальный анализ, возможно, по отдельным частям сферы действия, и, возможно, с использованием иного метода.

В стандартах, описывающих вопросы управления рисками информационной безопасности, отмечается, что каждая организация вправе выбирать свой подход к оценке рисков информационной безопасности, исходя из ее целей и задач.

После оценки рисков информационной безопасности получается список оцененных рисков информационной безопасности с их приоритетами, присвоенными в соответствии с критериями оценивания рисков информационной безопасности.

Оценка рисков информационной безопасности может проводиться не только на уровне организации или предприятия, в рамках взаимосвязанной совокупности систем, для отдельной системы или приложений, но и для конкретных критических функций внутри системы. Необходимо учитывать, что оценка рисков информационной безопасности на уровне организации не является простой комбинацией рисков для всех ее критических функций, поскольку совместное проявление нескольких рисков может существенно повысить общий риск информационной безопасности.

Для устранения выявленных рисков, предприятия должны внедрять стратегию информационной безопасности за счет создания всеобъемлющей структуры, кроме того, эта стратегия должна быть частью общих стратегических планов организации и поддерживаться первым лицом компании.

УДК 004.056

Остапенко Ирина Николаевна,
к.э.н., доцент
Усенко Роман Станиславович,
старший преподаватель
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

О МЕТОДИКАХ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

На сегодняшний момент не вызывает сомнений необходимость затрат в обеспечение информационной безопасности (ИБ) любой современной организации. Её потенциально уязвимые информационные активы – информация / данные, документы, аппаратные средства, программное обеспечение (ПО), оборудование для обеспечения связи, программно-аппаратные средства, продукция или услуги (например, информационные, вычислительные услуги), конфиденциальность и доверие при оказании услуг, оборудование, обеспечивающее необходимые условия работы, персонал организации, её имидж (он подвергаются риску, если по отношению к ним существуют какие-либо угрозы). Информационные риски зависят от ценности информационного ресурса (ИР), вероятности реализации угроз для ИР, эффективности предпринимаемых или планируемых средств обеспечения ИБ.

Одним из основных вопросов современной ИБ является вопрос оценки необходимого уровня затрат в ИБ для обеспечения максимального эффекта от вложений. Для решения этого вопроса необходимо применять системы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков, например, выраженных в виде ущерба, к затратам на ИБ).

Современные информационные технологии разрабатываются более высокими темпами, чем рекомендательная и нормативно-правовая база руководящих документов, действующих на территории Российской Федерации, поэтому актуальной остаётся проблема в выборе критериев и показателей, по которым оценивается эффективность системы защиты ИР, и обеспечивается оценка и мониторинг информационных рисков в организациях. В современной практике существуют разнообразные методики, используемые для разработки систем анализ рисков. Условно их можно разделить на следующие основные группы: количественные, качественные и методики, использующие смешанные оценки.

Количественная оценка рисков целесообразна, когда выявленным угрозам и связанным с ними рискам можно поставить в соответствие конечные количественные значения (в у.д.е., %, времени и т.п.). Процесс получения данных значений должен быть максимально прозрачен и доступен для понимания. Количественные методы базируются на следующих подходах: экспертный, вероятностно-статистический, нечёткой логики.

Таблица 1

Наиболее известные программные продукты анализа и оценки информационных рисков

Метод оценки рисков	Название программного обеспечения	Краткая характеристика программного обеспечения
Количественный	RiskWatch (США)	RiskWatch является американским стандартом в области анализа и управления рисками и ориентирована на точную количественную оценку соотношений потерь от угроз безопасности и затрат на создание системы защиты. Аналогично методу CRAMM, RiskWatch использует в качестве критериев для оценки и управления рисками предсказания годовых потерь (Annual Loss Expectancy – ALE) и оценку возврата от инвестиций (Return on Investment – ROI).
Качественный	РискМенеджер (Институт системного анализа РАН))	Система «РискМенеджер-Анализ» автоматизирует: - Построение моделей угроз, моделей событий рисков, оценки рискообразующих потенциалов угроз, объектов, организационных структур, бизнес-процессов; - Построение моделей защиты, моделей влияния средств защиты на изменение безопасности системы, расчета рископонижающих потенциалов мер защиты, выбора наиболее эффективных комплексов мер защиты по критерию эффективность-стоимость; - Расчет рисков нарушения безопасности, расчет остаточных рисков после применения возможных вариантов комплексов мер защиты; - Контроль качества требований к безопасности системы на актуальность, полноту, непротиворечивость; отсутствие дублирования, влияния на конкурентоспособность организации и обоснование внесения изменений в системы требований к безопасности.
Качественный и количественный	CRAMM (Великобритания)	Метод анализа и управления рисками CRAMM и соответствующий программный инструментарий, является правительственным стандартом Великобритании и широко распространен во всем мире. CRAMM реализует комплексный подход к оценке рисков, сочетая количественные и качественные методы оценки. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора. Версии ПО CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций – Правительственный профиль (Government profile).

Качественная оценка применяется, когда из-за большой степени неопределённости невозможно получить конкретное количественное выражение ИР как объекта оценки. При качественном подходе объекту оценки может присваиваться показатель, проранжированный по определённой балльной шкале. Для сбора данных в этом случае применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи и т.п. Проводится такой анализ с

привлечением экспертов, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Как правило, любая методика предполагает следующие этапы: идентификация активов, определение риска несоответствия требований законодательства в области ИБ, разработка модели угроз, процедура оценки рисков ИБ, определение допустимого уровня риска.

Краткая характеристика наиболее распространенных программных продуктов применительно к методикам анализа и оценки информационных рисков приведена в таблице 1.

УДК 338.242.2: 004. 056. 5

Смигельских Дмитрий Александрович
магистрант
Остапенко Ирина Николаевна
к.э.н., доцент
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Институт экономики и управления
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА РАЗЛИЧНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ИННОВАЦИИ

Непрерывное развитие экономики в современных условиях ставит инновационную деятельность на лидирующие позиции. Конкурентоспособность государства во многом определяется степенью и уровнем развития инновационной сферы. Актуальным становится вопрос рассмотрения обеспечения информационной безопасности (ИБ) на различных этапах жизненного цикла инновации с целью обеспечения высоких конкурентных преимуществ на рынке. Жизненный цикл инновации представлен на рисунке 1.

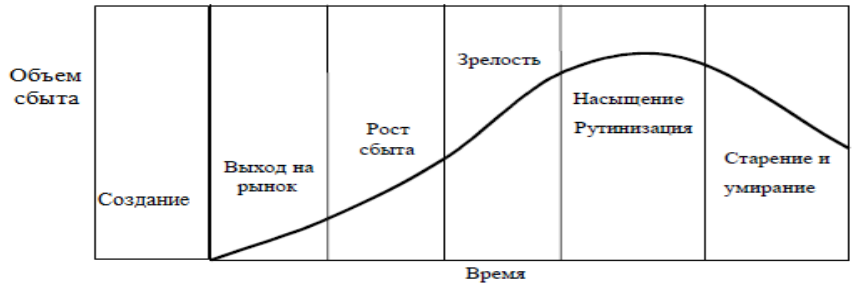


Рис. 1. Жизненный цикл инновации

На первом этапе создания инновации обеспечение ИБ играет ключевую роль. Она включает в себя защиту инженерно-технической и организационно - правовой информации. В том случае, если инновация представляет собой информационный продукт, то здесь важно отметить программные средства защиты от постороннего вмешательства конкурентов, а также криптографические методы защиты разработчиков продукта. Необходимо формирование будущей внутрифирменной стратегии ИБ в соответствии с направлением деятельности компании. Следующий этап – выход инновации на рынок. На данном этапе проводятся мероприятия по комплексному анализу маркетинга, включающего в себя анализ имеющегося потенциала предприятия, анализ потенциальных конкурентов и целевого рынка инновационного продукта, рассмотрение слабых и сильных сторон товара и оценка рисковой составляющей. ИБ в виде различных программных средств должна реализовать защиту собранных данных, доступ к которым имеет лишь ограниченный круг лиц. Последующие этапы – рост сбыта, зрелость и насыщение представляют собой периоды высокой доли присутствия инновации на рынке. Обеспечение ИБ на данных этапах служит одним из инструментов максимального использования имеющегося потенциала организации, получения высоких прибылей от продаж. Последний этап жизненного цикла – это старение и умирание, когда на рынке наблюдается резкий спад покупательской способности инновации. После этого жизненный цикл следует начинать заново с создания новой инновации или же усовершенствования уже имеющейся. В задачи ИБ на заключительном этапе входит сохранение в тайне имеющихся технологий создания инновации, различных отчетов о продажах и маркетинговых исследованиях, а также планов по усовершенствованию продукции. Все мероприятия по ИБ разрабатываются и контролируются службой защиты информации, которая для каждого предприятия сугубо индивидуальна, поскольку специфична сама инновационная деятельность.

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

СЕКЦИЯ 6.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТ-СИСТЕМАХ

СЕКЦИЯ 7.
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В МОБИЛЬНЫХ СИСТЕМАХ

СЕКЦИЯ 8.
ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР, ПОЛЬЗОВАТЕЛЕЙ, ИХ ДАННЫХ И ИНТЕРЕСОВ

СЕКЦИЯ 10.
МЕНЕДЖМЕНТ ИННОВАЦИЙ В СФЕРЕ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В ЭКОНОМИЧЕСКОЙ СФЕРЕ

Научное издание

Проблемы информационной безопасности

Труды III Международной научно-практической конференции

Симферополь – Гурзуф, 16-18 февраля 2017 г.

Ответственный редактор О. В. Бойченко

Компьютерная верстка М. А. Бакуменко

Подписано в печать 07.02.2017 г.
Формат 60x90/8. Бумага офсетная. Гарнитура Times New Roman.
Усл. п.л. 23,75. Количество экз. 150. Заказ № 10

Издатель ИП Зуева Т.В.
297565, Республика Крым, Симферопольский р-он, с. Кизиловое,
ул. Верхне-Кизиловая, д. 2, кв. 61

Отпечатано ИП Зуева Т.В.
295000, Республика Крым, г. Симферополь, ул. Тренева, 1

УДК 004.056:621.391
ББК 32.972.53
П781

ISBN 978-5-9908989-1-2