МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Кафедра теоретической экономики

КУРСОВАЯ РАБОТА

Безопасность информации в информационных системах

Работу выполнил _____ А.А. Гонин

(подпись, дата)

Факультет экономический Курс 3

Направление подготовки 38.03.05 – Бизнес-информатика

Профиль подготовки Электронный бизнес

Научный руководитель:

канд. экон. наук, доцент _____И.В. Богдашев

(подпись, дата)

Нормоконтролер:

канд. экон. наук, доцент _____И.В. Богдашев

(подпись, дата)

Краснодар 2018

Содержание

ВВЕДЕНИЕ

Безопасность информации, является одним из самых острых и приоритетных вопросов. Системы защиты информации очень востребованы, как среди государственных и коммерческих организаций, так и в жизни всего современного общества в целом. Электронные торговые площадки и сетевые предприниматели нуждаются в защите конфиденциальной информации и в снижении вероятности её кражи. Для большинства информационных систем свойственны некоторые факторы, которые могут создать уязвимости: большой объем информации, внушительное количество пользователей в системе, которые работают с данной информацией, анонимность доступа, передача информации по каналам связи, а также возможность «информационных диверсий». Все эти и многие другие факторы создают задачу поддержания безопасности информационных сетей.

Важную роль в деятельности по защите информации и информационных систем занимают мероприятия по созданию комплексной защиты. На данный момент ни одна система защиты не обеспечивает стопроцентную безопасность, в следствии возможности её взлома и поиска «программных дыр». Поэтому требуется проанализировать особенности и состояние не только отечественной информационной безопасности, но и мировой, а также сформулировать оптимальную модель информационной безопасности, нашей страны и определить возможности её реализации. Таким образом *тема является актуальной* в современных условиях.

Данная работа посвящена проблеме обеспечения информационной безопасности в электронных информационных системах

Целью работы является выявление и устранение источников угроз для информации, поиск причин и условий, способствующих нанесению финансового, материального ущерба, а также поиск способов по их устранению и описание данных способов.

Для достижения этих целей необходимо:

- Рассмотреть теоретические аспекты защиты информационных систем;

- Изучить методы и средства защиты информации;

- Рассмотреть возможности программного обеспечения по поддержанию безопасности.

Предметом исследования выступает состояние и методы обеспечения информационной безопасности в современных условиях.

Объектом исследования является информация безопасность государства в целом, и сама информация как неотъемлемая часть современной инфраструктуры общества.

Научная значимость рассматриваемой темы обусловлена её важностью исследования и изучения, так как проблема формирования информационной безопасности в нашей стране, разработка новейших методов реализации этой проблемы является сегодня важнейшей задачей для специалистов в области мировой политики, политологии и социологии, а так же в сфере бизнеса и предпринимательства.

Методологическую базу составляют: методы комплексного и системного анализа на основе междисциплинарного исследования актуальных проблем (основных понятий, предмета, структуры информации и безопасности, а также отношений, возникающих, в связи с этим и их отражением в праве и законодательстве России); общенаучные методы познания и др.

Информационная база исследования послужили труды отечественных экономистов и программистов таких, как Стрельцов, А.А., Конявский, В.А., Раткин, Л.С. и др., а также справочные материалы,

нормативные документы, законодательные акты и Интернет-ресурсы.

Курсовая работа включает в себя: введение, глава 1, глава 2, заключение, список использованных источников. В первой главе рассматриваются виды информационных систем и возможные угрозы и соответственно их источники. Вторая глава включает в себя исследование основных проблем и перспектив информационной безопасности, способов и методов её обеспечение, а также прогноз развития данной сферы в будущем.

1: Защита информации и информационная безопасность

1.1 Виды информационных систем

Начать стоит с того, что под информационной безопасностью понимается комплекс организационных и технических мер, которые принимаются для обеспечения защиты, целостности, доступности и управляемости массивов информации. В рамках общей концепции безопасности государства информационная безопасность обеспечивает связанное взаимодействие всех элементов системы. [4] Структурные элементы информационной безопасности на международном и внутригосударственном уровне включают:

- защиту сведений, содержащих государственную или коммерческую тайну;
- защиту серверов государственных учреждений и систем жизнеобеспечения;
- защиту безопасности данных как набор аппаратных и программных средств, которые обеспечивают сохранность информации от неавторизированного доступа, затруднения доступа, разрушения и перепрограммирования;
- информационно-психологический блок, который подразумевает реализацию системы мер, направленных на защиту от целенаправленного информационного воздействия на субъект нападения, его психологическое состояние или имидж на международной арене.

Защита всех составляющих требует разработки методического аппарата и создания собственной инфраструктуры. Задачи обеспечения информационной безопасности осложняются тем, что информационное пространство не имеет границ. Особенности работы сети Интернет и возможности беспроводной связи создают предпосылки для бесконтрольного и беспрепятственного переноса через рубежи государств огромных массивов данных, часто содержащих

сведения, оборот которых в мире или в отдельных странах запрещен или ограничен.

Что же такое информация? Можно сказать, что информация – это в первую очередь сведения, передаваемые людьми различными способами, к примеру письменным или устным. С середины 20-ого века, информация становится общенаучным понятием. В рамках нашей дисциплины, под информацией можно понимать сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах. [5]

Информационная система – это система, предназначенная для хранения, поиска и обработки информации. Так же можно сказать, что информационная система предназначена для своевременного обеспечения надлежащих людей надлежащей информацией, то есть для удовлетворения конкретных информационных потребностей в рамках определенной предметной области, при этом результатом функционирования информационных систем является информационная продукция — документы, информационные массивы, базы данных и информационные услуги. [3]

Виды информационных систем так же разнообразны, как виды деятельности людей и их ассоциаций. Информационные системы, как организованная система информации и ее обработки, создаются на основе двух определяющих условий. Система формируется либо на базе информации, которой обладает ее создатель, т.е. по принципу источника, авторской принадлежности, либо на основе учета интереса и потребности пользователя в определенном виде информации, которая пополняется и изменяется по ходу реализации потребности. [6]

В настоящее время информационные системы по статусу их создателей и целевому назначению можно систематизировать следующим образом:

1) Персональные компьютерные системы, аккумулирующие данные по интересу и потребности пользователя;

2) Локально-целевые, создаваемые внутри организации для выполнения определенных функций или операций. Например, регистрация обслуживаемых в поликлинике; системы контроля за исполнением решений в органе власти и т.п.;

3) Внутриведомственные, или корпоративные, системы, объединяющие базы и банки данных по кругу своих профессиональных или производственных обязанностей;

4) Региональные и межрегиональные справочные, регистрационные, учетные, аналитические и иные системы. Например, центры открытого доступа в муниципальных образованиях, в субъекте РФ;

5) Базы и банки данных многофункциональных информационных центров (МФЦ) по обслуживанию систем "одного окна" в области предоставления услуг населению;

6) Государственные территориально распределенные системы программного назначения – электронное управление (правительство), или системы в области оперативно-розыскной деятельности. Такие системы интеграционного и аналитического назначения пересекаются с упомянутыми в п. 6;

7) Межгосударственные автоматические системы управления. Например, АСУ таможенного союза, системы розыска пропавших лиц, системы розыска преступников и т.п.

1.2 Виды возможных угроз информационной безопасности

Под термином информационная безопасность, опираясь на Доктрину информационной безопасности Российской Федерации, понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. Можно сказать, что информационная безопасность – это защита информации от случайных или преднамеренных воздействий

естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю. [27]

Стоит обратить внимание, что информационная безопасность – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы. Безопасной информационной системой можно назвать систему, которая, во-первых, защищает данные и информацию от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надежно хранит информацию и гарантирует неизменность данных. То есть система должна обладать такими свойствами как конфиденциальность, доступность и целостность.

Возникновение новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. [1]

Спустя какое-то время, защита экономической информации стала обязательной: были разработаны всевозможные документы по защите информации; сформировались рекомендации по защите информации; так же проводится ФЗ о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации. [27]

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

Под угрозой информационной безопасности понимается потенциально возможные действия или же процессы, которые способны оказать нежелательные воздействия на саму систему или информацию, находящуюся в

ней. Такие угрозы могут привести к искажению, копированию, незаконному распространению или же ограничению доступа к данным системы.

Виды угроз информационной безопасности очень разнообразны и имеют множество разновидностей, но я выделю самые главные на мой взгляд:

1. По природе возникновения: Естественные и искусственные.

К видам естественных угроз, относятся угрозы, связанные с возникновением и воздействием физических процессов или природных, стихийных явлений на компьютерную систему. Искусственные угрозы подразумевают влияние деятельности человека и разделяются на непреднамеренные угрозы (случайные), к примеру различные неполадки программного обеспечения, ошибки персонала, или же ситуацию в которой вычислительная и коммуникативная техника приходит в негодность, и на преднамеренные угрозы (умышленные), например несанкционированный доступ к информации, создание различных, специализированных программных продуктов, целью которых является осуществление неправомерного доступа, а так же разработка и внедрение вирусных программ.

2. По аспекту информационной безопасности, на который направлены угрозы:

Первый аспект, это угроза конфиденциальности, то есть получение доступа к информации третьих лиц, не располагающих полномочиями для доступа к ней. В данном случае используют такой термин как «утечка информации». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств. [1]

Следующим можно выделить угрозу целостности. Это угроза, связанная с возможностью модификации, редактированию той информации которая хранится в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.

Заключительным аспектом можно выделить угрозу доступности. Данная угроза представляет собой создание таких условий, при которых доступ к информации или услуге будет либо затруднен, либо полностью заблокирован.

3. По размерам наносимого ущерба:

- Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);
- Локальные (причинение вреда отдельным частям объекта безопасности);
- Частные (причинение вреда отдельным свойствам элементов объекта безопасности).

Нельзя оставить без внимания угрозы, связанные с вредоносным программным обеспечением. Вредоносной программой называется любое программное обеспечение, целью которого является неправомерное получение доступа к информации, находящейся на компьютере, электронном носителе или же в информационной базе данных, с целью порчи или хищения данных.

Вредоносное программное обеспечение, направленное на нарушение системы защиты информации от несанкционированного доступа можно классифицировать по следующим критериям:

1) Логическая бомба. Инструмент уничтожения или нарушения целостности информации, однако, иногда ее применяют и для кражи данных. Логическая бомба – это серьезная угроза. Как правило предприятие редко способно справится с такой атакой, связано это с тем, что подобные манипуляции проводятся недовольными служащими, а также сотрудниками с особыми политическими взглядами. Из этого следует вывод, что большинство организаций не готовы к непредсказуемой угрозе, где главную роль несет человеческий фактор.

2) Троянский конь – это программа, запускающийся к выполнению дополнительно к другим программным средствам защиты информации и прочего ПО, необходимого для работы.

Если говорить более точно, программа обходит систему защиты с помощью выполнения недокументированных действий.

3) Вирус – это специальная самостоятельная программа. Характерными чертами является способность к самостоятельному распространению по системе, размножению и внедрению своего кода в сторонние программы путем изменения данных с целью выполнения вредоносного кода не оставляя «следов».

Вирусы характеризуются тем, что они способны самостоятельно размножаться и вмешиваться в вычислительный процесс, получая возможность управления этим процессом.

То есть, если Ваша программное аппаратная защита информации пропустила подобную угрозу, то вирус, получив доступ к управлению информационной системой, способен автономно производить собственные вычисления и операции над хранящейся в системе конфиденциальной информацией.

4) Червь – программа, передающая свое тело или его части по сети. Не оставляет копий на магнитных носителях и использует все возможные механизмы для передачи себя по сети и заражения атакуемого компьютера.

5) Перехватчик паролей – программный комплекс для воровства паролей и учетных данных в процессе обращения пользователей к терминалам аутентификации информационной системы.

Программа не пытается обойти службу информационной безопасности напрямую, а лишь совершает попытки завладеть учетными данными, позволяющими, не вызывая никаких подозрений совершенно санкционировано проникнуть в информационную систему, минуя службу информационной безопасности, которая ничего не заподозрит. Обычно программа инициирует ошибку при аутентификации, и пользователь, думая, что ошибся при вводе пароля повторяет ввод учетных данных и входит в систему, однако, теперь эти данные становятся известны владельцу перехватчика паролей, и дальнейшее использование старых учетных данных небезопасно.

Важно понимать, что большинство краж данных происходят не благодаря хитроумным способам, а из-за небрежности и невнимательности, поэтому понятие информационной безопасности включает в себя: информационную безопасность (лекции), аудит информационной безопасности, оценка информационной безопасности, информационная безопасность государства, экономическая информационная безопасность и любые традиционные и инновационные средства защиты информации. [5]

Публикации последних лет говорят о том, что техника защиты информации не успевает развиваться за числом злоупотреблений полномочиями, и техника защиты информации всегда отстает в своем развитии от технологий, которыми пользуются взломщики для того, чтобы завладеть чужой тайной.

Существуют документы по защите информации, описывающие циркулирующую в информационной системе и передаваемую по связевым каналам информацию, но документы по защите информации непрерывно дополняются и совершенствуются, хотя и уже после того, как злоумышленники совершают все более технологичные прорывы модели защиты информации, какой бы сложной она не была.

Сегодня для реализации эффективного мероприятия по защите информации требуется не только разработка средства защиты информации в сети и разработка механизмов модели защиты информации, а реализация системного подхода или комплекса защиты информации – это комплекс взаимосвязанных мер, описываемый определением «защита информации». Данный комплекс защиты информации, как правило, использует специальные технические и программные средства для организации мероприятий защиты экономической информации.

2: Проблемы и перспективы защиты информации и обеспечения информационной безопасности

2.1 Способы и средства информационной безопасности: мировой и российский опыт

Важность и сложность проблемы защиты информации, создает необходимость создания политики информационной безопасности, которая подразумевает ответы на следующие вопросы:

- Какую информацию защищать?
- Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?
- Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты?
- Какие средства использовать для защиты каждого вида информации?

Одним из главных пунктов обеспечения безопасности, является предоставление каждому сотруднику предприятия того минимального уровня привилегий доступа к базе данных и информационной системе, который необходим им для выполнения должностных обязанностей. При условии, что большинство нарушений в области безопасности исходит именно от собственных сотрудников, введение четких ограничений является очень важным условием.

Рассматривая методы защиты информации, можно выделить следующие, наиболее распространенные:

В первую очередь я бы выделил такую науку как криптография. Это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает решения многих проблем информационной

безопасности сети: аутентификация, конфиденциальность, целостность и контроль взаимодействующих участников.

Термин «Шифрование» означает преобразование данных в форму, не читабельную для человека и программных комплексов без ключа шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. Ключ – это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Одной из основ информационной безопасности криптографии является целостность данных. Защита информации в локальных сетях и технологии защиты информации наряду с конфиденциальностью обязаны обеспечивать и целостность хранения информации. То есть, защита информации в локальных сетях должна передавать данные таким образом, чтобы данные сохраняли неизменность в процессе передачи и хранения.

Для того чтобы информационная безопасность информации обеспечивала целостность хранения и передачи данных необходима разработка инструментов, обнаруживающих любые искажения исходных данных, для чего к исходной информации придается избыточность.

Информационная безопасность в России с криптографией решает вопрос целостности путем добавления некой контрольной суммы или проверочной комбинации для вычисления целостности данных. Таким образом, снова модель информационной безопасности является криптографической – зависящей от ключа. По оценке информационной безопасности, основанной на

криптографии, зависимость возможности прочтения данных от секретного ключа является наиболее надежным инструментом и даже используется в системах информационной безопасности государства.

Следующим методом защиты информации является экранирование. Экран, или же брандмауэр – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем.

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует. В более общем случае экран или полупроницаемую оболочку удобно представлять себе, как последовательность фильтров. Каждый из них может задержать данные, а может и сразу "перебросить" их "на другую сторону". Кроме того, допускаются передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа экраны осуществляют также протоколирование информационных обменов.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны устанавливают для защиты локальной сети организации, имеющей выход в открытую среду, подобную The Internet.

Экранирование позволяет поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, индуцированную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие

от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности.

Экранирование - один из наиболее действенных способов защиты информации, но бывают и непредсказуемые ситуации. Дело в том, что большинство межсетевых экранов требуют для своей полноценной и корректной работы административных прав. А ведь очень много экранов имеют уязвимости. Воспользовавшись одной из таких уязвимостей, хакер без труда получит права, под которыми работает экран и получит любые права для управления и изменения информационной системы предприятия или организации. [27]

Ещё одним аспектом информационной защиты на предприятии, является работа с персоналом. В сферу действия обеспечения информационной безопасности попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика защиты ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего требованиям нормативных документов;

- исследование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности)

- обеспечение безопасности в каждой функциональной области локальной сети;

- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;

- обеспечение анализа регистрационной информации;

- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности

- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;

- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Одним из главных пунктов работы с персоналом и создание благоприятных условий для развития информационной безопасности компании, является правильное распределение ролей.

Перечисленные ниже группы людей отвечают за реализацию сформулированных ранее целей.

- руководитель организации отвечает за выработку соответствующей политики обеспечения информационной безопасности и проведение ее в жизнь;

- руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними;

- администраторы сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики обеспечения информационной безопасности;

- пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Нарушение политики обеспечения информационной безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Поскольку наиболее уязвимым звеном любой информационной системы является человек, особое значение приобретает

воспитание законопослушности сотрудников по отношению к законам и правилам информационной безопасности. Случаи нарушения этих законов и правил со стороны персонала должны рассматриваться руководством для принятия мер, вплоть до увольнения.

Информационная безопасность в России рассматривается на уровне Доктрины информационной безопасности, которая служит основой для принятия нормативных актов. Среди фундаментальных вопросов доктрины – необходимость самостоятельного информационного присутствия России в международном сообществе и выбор каналов поставки достоверных данных и новостей, что позволит снизить ущерб от дезинформационных атак.

За информационную безопасность России на современном этапе отвечают различные государственные учреждения, в том числе Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), специализированные подразделения министерств и ведомств, а также межведомственная комиссия при Совете Безопасности. Однако участники процесса борьбы с кибератаками считают, что на современном этапе необходимо объединить функции и передать отдельному регулятору уровня федеральной службы с самостоятельными ресурсами и значительными полномочиями. [4]

Пока российская система переживает стадию роста и отвечает не всем требованиям, позволяющим обеспечить ИБ в полном объеме. Причин несколько:

1) Независимость – это, если говорить точнее, информационная самостоятельность государства, отсутствие зависимости от зарубежного программного обеспечения и методов обеспечения защиты в пользу отечественных. Важный аспект обеспечения независимости – создание четко выстроенной системы межведомственного взаимодействия и самостоятельной структуры для управления рисками с опорой на нормативно-правовую базу, что обеспечит полномочия и возможности для работы. Существенной проблемой

становится и отсутствие собственной аппаратной части, что ставит систему информационной безопасности России в положение зависимости от иностранных поставщиков. [12, с. 27]

2) Слабая защищенность финансовой системы – то есть отсутствие высокого уровня защиты у различных секторов экономики, таких как финансы властных структур, финансы крупных предприятий, финансы субъектов Федерации и др. Уязвимыми элементами ИБ в российском финансовом секторе остаются нехватка квалифицированных специалистов, программное обеспечение и недостаточная координация с правоохранительными органами. [4]

Из стран мира с развитой информационной безопасностью можно выделить: Великобританию, Францию, Германию.

В Великобритании информационной безопасностью занимаются уже давно, но из этого выливается проблема консервативности методов. Разработанная когда-то система остается неизменной уже достаточно давно. Между тем в области информационных технологий все меняется очень быстро, так что периодически возникает необходимость в определенной коррекции органов защиты данных.

Франция выделяется тем, что внутри страны действует огромное количество частных организаций, которые разрабатывают, устанавливают и обслуживают комплексные системы защиты информации. Они, несмотря на свою независимость, очень тесно сотрудничают с соответствующими отделами полиции. Это позволяет правоохранительным органам быстро реагировать на любые правонарушения и пресекать их. Еще одной особенностью французской организации системы защиты информации является ее правовое обеспечение. Дело в том, что в этой стране нет специальных правовых актов, регулирующих работу людей с различными видами информации. Безопасность государственной тайны гарантируется уголовным, а персональной и коммерческих тайн - уголовным, трудовым и гражданскими кодексами.

Германия - одна из самых "продвинутых" в области информационной безопасности стран Западной Европы. Она обладает развитой структурой органов, заботящихся о защите различных видов тайн. Первоначальной задачей этих структур была защита от промышленного шпионажа и охрана государственных секретов. Кроме того, очень большую пользу приносит федеральное ведомство по обеспечению безопасности в сфере информационной техники. В задачу этой организации входит координирование работы других структур по защите данных, сертификация и стандартизация средств безопасности. Кроме того, ведомство занимается пропагандой необходимости защиты данных, а также оказывает консультационные услуги в этой области.

2.2 Прогноз развития технологий защиты информации и программного обеспечения от вредоносного воздействия

Тенденция развития традиционного рынка ИБ показывает, что для него характерно отставание от IT сферы в плане развития. Появляются новые технологии, которые провоцируют новые угрозы, а вслед за этим рождаются новые способы борьбы и защиты. Несмотря на тот факт, что уровень IT рынка на российской арене довольно сильно уступает Западу, все же серьезного отставания в сфере информационной безопасности, не наблюдается. Можно заметить, что как в России, так и на Западе, по большей части используется одно и то же программное и аппаратное обеспечение – антивирусные системы, брандмауэры, системы предотвращения межсетевых атак и т.д. Во многом это связано с тем, что до последнего момента информационная безопасность рассматривалась представителями отечественного бизнеса как сугубо техническая область, а все возникающие проблемы решались путем применения новейших технических средств. Однако на Западе исторически система управления и менеджмента развита намного сильнее, большинство

компаний подходят к ИБ как к процессу, которым необходимо управлять для его увязки с бизнесом в целом. [8, с.112]

Примерный прогноз развития данного рынка можно представить ссылаясь на ежегодно проводимую конференцию в России «Академия информационных систем». В ходе данной конференции были выделены основные направления, которые должны оказаться в фокусе внимания разработчиков самых популярных компаний, связанных с информационной безопасностью. Из разработок можно выделить:
1) Модернизация межсетевых экранов. По-прежнему это наиболее эффективные инструменты для защиты от сетевых атак. В будущем в связи с ростом пропускной способности сети и объемов трафика, стоит ждать серьезного улучшения данного вида продукции.

2) Рост интернет-доступа. В связи с тем, что сеть интернет распространяется с огромной скоростью и стал доступен практически каждому, увеличивается и количество атак, что потребует особого внимания со стороны компаний по обеспечению информационной безопасности.

3) Открытые сети. Полностью закрыть свои информационные ресурсы от доступа партнеров или клиентов зачастую попросту невозможно. И в этом случае возникают серьезные проблемы безопасности: требуется четкое разграничение доступа к той или иной информации. Эта важная проблема с точки зрения ИБ требует новых технических решений.

4) Уязвимость встроенных операционных систем в мобильных телефонах, банкоматах и автомобильных компьютерах - пока что редкие мишени для злоумышленников. Последствия от атак на эти системы в комментариях не нуждаются, и уже сегодня необходимо готовиться к тому, что в ближайшие два года число несанкционированных действий в данной области будет стремительно расти.

5) Стандарты ИБ. Стандартизация, которая приходит из IT в информационную безопасность, это правильный и необходимый процесс, который позволяет специалистам и регулирующим органам общаться на одном

языке, а также определяет минимальный уровень систем безопасности компаний различных отраслей.

Международный сервис-провайдер Orange Business Services и исследовательская компания International Data Corporation (IDC) в феврале 2018 года сообщили о проведении анализа корпоративного рынка услуг кибербезопасности в России. В рамках исследования компаний были изучены многие сегменты такие, как управляемые услуги безопасности и управляемые удаленные услуги безопасности, облачные корпоративные услуги безопасности и консалтинговые услуги.

Исходя из исследований, проведенных компанией IDC, можно увидеть, что суммарный объем приведенных выше сегментов рынка в 2016 году, достиг высокой отметки в $81,88 млн, что составляет 58,2% от общего объема корпоративного рынка услуг безопасности в РФ. Судя по прогнозу аналитиков, объем рынка корпоративных услуг безопасности может приблизится к 6 млрд рублей в 2021 году, а к 2022 году среднегодовой темп роста упомянутых сегментов составит 3,9%. Рынок услуг все больше стимулирует рынок информационной безопасности и продолжает привлекать новых игроков, раннее известных в других ИТ-сферах. [11]

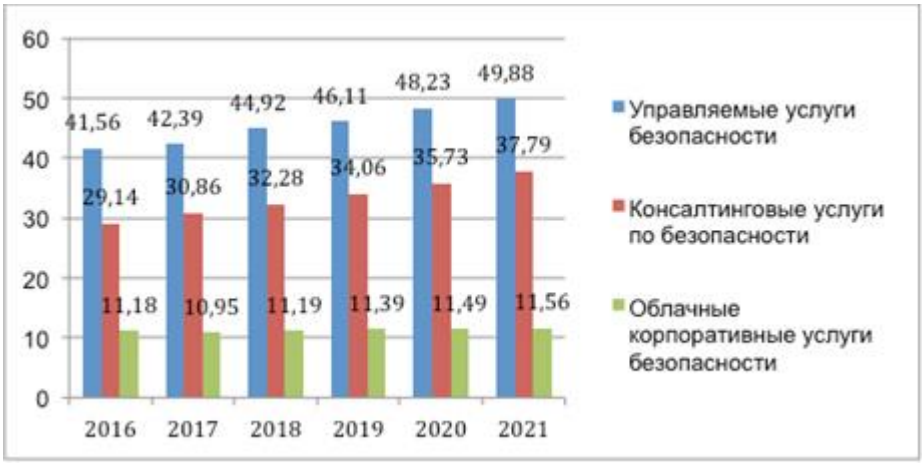

Рисунок 1 - Объем и прогноз развития российского рынка услуг безопасности, (млн долларов)

Исследуя рисунок 1, можно прийти к выводу, что с расчётом на ближайшие 5 лет, наиболее высокие темпы роста ожидаются от рынка консалтинга по безопасности. Согласно прогнозу, среднегодовой темп роста

тестирования на проникновение и уязвимости достигнет 4,7%, в то время как планирование стратегии безопасности покажет еще более внушительные результаты — 5,9%.

Именно консалтинг способствует увеличению прозрачности внутренних процессов предприятия и снижению дефицита квалифицированных кадров.

Следовательно, можно сделать вывод, что финансовый сектор будет оставаться лидером по спросу на услуги ИТ-безопасности, в связи с тем, что большинство самых сложных и продвинутых атак злоумышленников за последние несколько лет были нацелены на финансовые учреждения. [11]

ЗАКЛЮЧЕНИЕ

Неотъемлемой частью современного общества выступает его информатизация – постоянная разработка, модернизация и внедрение информационных систем во все сферы человеческой деятельности. Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Обширные возможности и средства компьютеров и информационных технологий, дают возможность автоматизации процессов мониторинга и управления как государственными, так и экономическими структурами, а также наделяет общество возможностью накапливать, обрабатывать и передавать информацию о важных процессах с высокой скоростью и в любом количестве.

В настоящее время информация считается стратегическим национальным ресурсом - одним из основных богатств страны. Потеря конфиденциальной информации приносит моральный или материальный ущерб.

Из проведенной работы становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Комплексная система защиты информации должна быть непрерывной, это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Информатизация общества несет в себе не только позитивные перемены, но и создает проблемы информационной безопасности, главные из которых – возникновение информационных войн и кибертерроризма. Эти проблемы носят глобальный характер, но вследствие геополитической и экономической ситуации приобретают особую остроту для России.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

В современном обществе информационная безопасность является важнейшим компонентом национальной безопасности. От нее в значительной степени зависит уровень экономической, оборонной, социальной, политической и других видов безопасности.

Выбор способов защиты информации в информационной системе - сложная оптимизационная задача, при решении которой требуется учитывать вероятности различных угроз информации, стоимость реализации различных способов защиты и наличие различных заинтересованных сторон. В общем случае для нахождения оптимального варианта решения такой задачи необходимо применение теории игр, в частности теории биматричных игр с ненулевой суммой, позволяющими выбрать такую совокупность средств защиты, которая обеспечит максимизацию степени безопасности информации при данных затратах или минимизацию затрат при заданном уровне безопасности информации.

В заключении хотелось бы добавить, что проблемы информационной безопасности многоаспектны и нуждаются в последующих исследованиях и разработках, и является одним приоритетных направлений развития.

Задачи, сформулированные во введении, решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1 Виды и источники угроз информационной безопасности [Электронный ресурс]. Режим доступа: http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti — 02.05.2018

2 Безопасность офиса. Современные решения [Электронный ресурс] / Д. А. Полухина // Директор по безопасности: электронный научный журнал. Режим доступа: http://www.s-director.ru/magazine/magdocs/view/136.html — 24.04.2018

3 Информационная система. Википедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/ Информационная_система - 02.05.2018

4 Роль информационной безопасности в современном мире [Электронный ресурс]. Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ib-v-rossii-i-mire/ — 02.05.2018

5 Средства обеспечения информационной безопасности от вредоносного ПО [Электронный ресурс]. Режим доступа: http://www.livesafety.ru/content/notes/information_security.php?ELEMENT_ID=1679 — 02.05.2018

5 Блинов, А.М. Информационная безопасность. Учебное пособие / А.М. Блинов. — СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

6 Информационное право. Статья: Виды информационных систем [Электронный ресурс]. Режим доступа: https://studme.org/57478/pravo/vidy_informatsionnyh_sistem — 02.05.2018

7 Приходько А. Я. Информационная безопасность в событиях и фактах / А. Я. Приходько – М.: СИНТЕГ, 2001. – С. 187-193.

8 Конявский, В.А Развитие средств технической защиты информации / В. А. Конявский // Комплексная защита информации. Сборник материалов XII Международной конференции (13-16 мая 2008 г., Ярославль (Россия)). М., 2008. С. 109-113.)

9 Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко – М.: Горячая линия-Телеком, 2000. – С. 232-245.

10 Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин, А. С. Кузьмин, С. Н. Смирнов – М.: Гелиос-АРВ, 2002. – С. 197-218.

11 Прогноз Orange Business Services и IDC до 2022 года [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России) – 02.05.2018

12 Малюк, А.А. Зарубежный опыт формирования в обществе культуры информационной безопасности / А.А Малюк, О.Ю Полянская// Безопасность информационных технологий. – 2016. – № 4. – С. 25-37.

13 Стрельцов, А.А**.** К вопросу о цифровом суверенитете **/** А.А Стрельцов, П.Л Пилюгин // Информатизация и связь. – 2016. – № 2. – С. 25-30.

14 Раткин, Л.С. Средства защиты информации как часть инфраструктурной системы глобальной национальной безопасности / Л.С. Раткин // Защита информации. Инсайд. – 2016. – № 4 (70). – С. 25-29.

15 Жарова, А.К. Правовая классификация угроз и рисков в информационной сфере / А.К. Жарова // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2016. – № 7-8 (97-98). – С. 130-138.

16 Об информации, информационных технологиях и о защите информации федер. закон от 27.07.2006 N 149-ФЗ

17 Об утверждении Доктрины информационной безопасности Российской Федерации Указ Президента РФ от 05.12.2016 N 646

18 О персональных данных федер. закон от 27.07.2006 N 152-ФЗ

19 Астахова, Л.В. Кадровые проблемы построения системы управления информационной безопасностью на предприятии / Л.В. Астахова, Л.О. Овчинникова // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 3 (21). – С. 38-46.

20 Защита информации от несанкционированного доступа [Электронный ресурс]. Режим доступа: http://bukvasha.ru/referat/393529 — 02.05.2018

21 Информационные технологии в профессиональной деятельности [Электронный ресурс]. Режим доступа: https://www.bibliofond.ru/view.aspx?id=863692 — 02.05.2018

22 Марков, Р.А. Подход к выявлению инцидентов информационной безопасности / Р.А. Марков, В.В Бухтояров, А.М. Попов; под ред. Р.А. Маркова // Научно-технический вестник Поволжья. – 2016. – № 1. – С. 78-80.

23 Остроух, Е.Н. Разработка методов и алгоритмов проверки работы предприятия с точки зрения информационной безопасности его функционирования / Е.Н. Остроух, Ю.О. Чернышев, С.А. Мухтаров; под ред. Е.Н Остроух // Инженерный вестник Дона. – 2016. Т. 41. – № 2 – (41). С. 31.

24 Полтавцева, М.А. Безопасность баз данных: проблемы и перспективы / М.А Полтавцева // Международный научно-практический журнал «Программные продукты и системы». – 2016. – №3. – С. 36-41.

25 Голубчиков, С.В. Уровни и правовая модель информационной безопасности / С.В. Голубчиков // Международный научно-практический журнал «Программные продукты и системы». – 2017. – №2. – С. 320-323.

26 Матвейкин, В.Г. Программно-алгоритмический комплекс защиты и управления предприятием / В.Г. Матвейкин, Б.С. Дмитриевский, В.И. Медников; под ред. В.Г. Матвейкина // Международный научно-практический журнал «Программные продукты и системы». – 2017. – №2. – С. 307-313.

27 Основы информационной безопасности и защиты информации [Электронный ресурс]. Режим доступа: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1 – 02.05.2018