Содержание:

Введение

Актуальность темы работы заключается в том, что в связи с вхождением общества в его информационную фазу развития, основанную на новейших наукоёмких технологиях, всё больше возникает необходимость предотвращения угроз информационной безопасности.

Угрозы, исходящие из различных источников, будучи неподконтрольными со стороны банков, могут оказывать дестабилизирующее воздействие на его деятельность. Например, бездействие в сфере защиты информации может привести к нарушению коммерческих интересов организации, вплоть до нанесения ему невосполнимых экономических потерь; снижения деловой активности или способности организации выступать в качестве конкурирующей стороны на товарных рынках; лишение предприятия научно-технического приоритета в соответствующих областях его деятельности; потеря деловой репутации и т.д.

Общее усиление компьютерной преступности в бизнесе (особенно в кредитно-финансовой сфере) напрямую связано с такими характеристиками Интернета, как легкая подключаемость к этой сети и возможность анонимного выполнения тех или иных незаконных действий.

Объектом исследования являются информационная безопасности в Российской Федерации на примере системы банкомата.

Предметом исследования являются виды и состав угроз информационной безопасности.

Цель исследования рассмотрение современной доктрины информационной безопасности в Российской Федерации.

Для достижения поставленной цели, в работе поставлены следующие исследовательские задачи:

1) Изучить виды и состав угроз информационной безопасности;

2) Выявить концепции определяющие природу информационной безопасности;

3) Провести разработку информационной системы безопасности на примере банкомата.

Методологическую основу исследования составляет широкий спектр методов в современной науке: общефилософские методы – диалектика и синергетика, общенаучные методы эмпирического и теоретического уровней, правовые частные и специальные методы.

Научная новизна исследования заключается в системном изучении сущности универсальных и специфических свойств информационной безопасности, выделении узловых проблем в системе информационной безопасности, требующих особого правового регулирования, определении концептуальных перспектив в области обеспечения современной доктрины информационной безопасности в Российской Федерации.

Структура работы состоит из введения, двух глав, заключения, библиографического списка и приложения.

Глава 1. Теоретические основы информационной безопасности

- 1. Виды и состав угроз информационной безопасности

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Фактор, воздействующий на защищаемую информацию - явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость информационной системы (брешь)- свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

По отношению к информации и информационным ресурсам можно выделить угрозы целостности, конфиденциальности, достоверности и доступности информации, проявляющиеся в различных формах нарушений (рис. 1.).

Как правило, вышеперечисленные угрозы информационным ресурсам реализуются следующими способами[1]

1. Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах, имеющих возможность получения конфиденциальной информации (суды, налоговые органы, коммерческие банки и т. д.).

2. Путем подкупа лиц, непосредственно работающих в организации или структурах, напрямую связанных с ее деятельностью.

3. Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике с помощью технических средств разведки и съема информации.

4. Путем прослушивания конфиденциальных переговоров и другими способами несанкционированного доступа к источникам конфиденциальной информации.

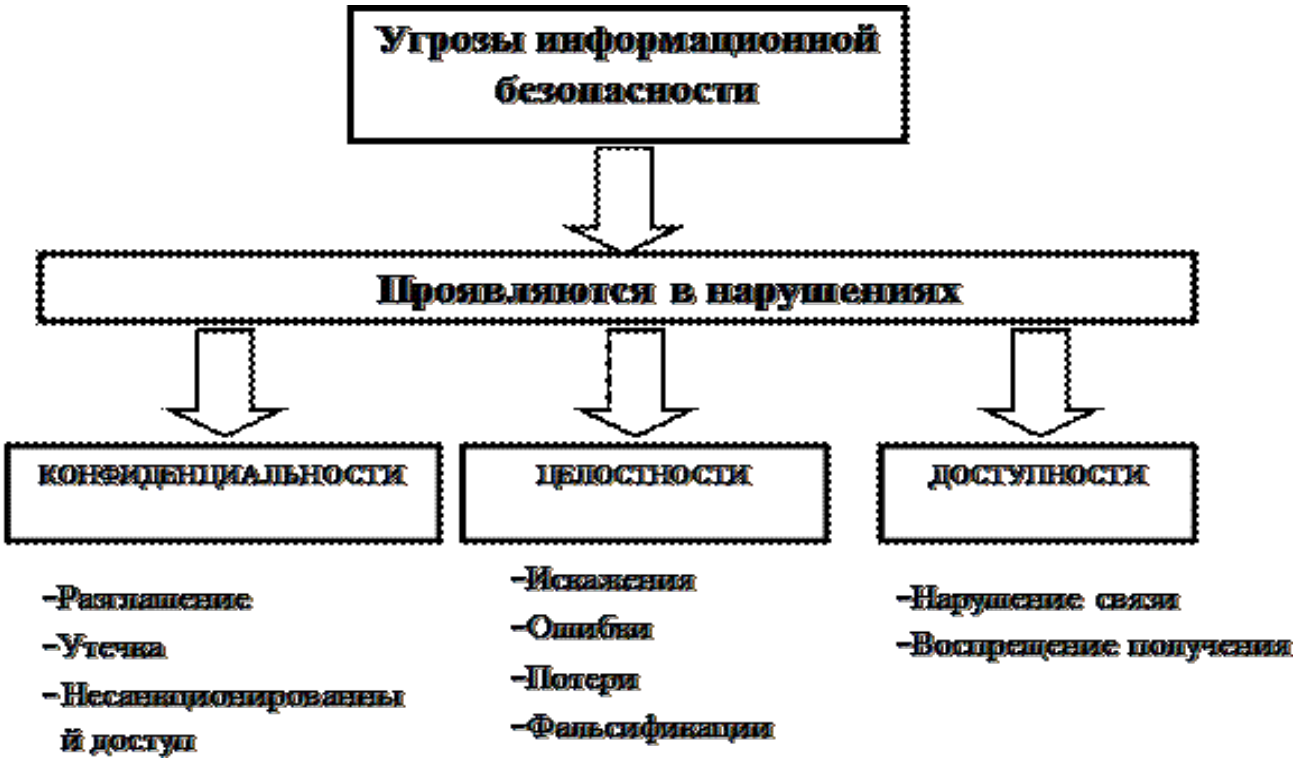


Рис. 1. Влияние угроз информации на критерии информационной безопасности

Информационная безопасность оказывает влияние на защищенность интересов в различных сферах жизнедеятельности общества и государства. В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности.[2]

Например, с позиции обеспечения безопасности информации в компьютерных системах(КС) все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными.[3]

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Информационная безопасность Российской Федерации — совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Легальное значение данного понятия содержится в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 г. № Пр-1895, согласно которой под информационной безопасностью Российской Федерации понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Доктрина представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности и служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации.

Анализ дефиниций «информационная безопасность», предложенных научными деятелями или закрепленных в нормативно-правовых актах, свидетельствует об определении ее в качестве «состояния защищенности национальных интересов в информационной сфере».[4]

Некоторые авторы обосновывают данное явление через наличие угрозы, т.е. определяют информационную безопасность как состояние защищенности национальных интересов в информационной сфере от внутренних и внешних угроз.

Один из подходов нашел свое отражение в работах ученых технического профиля. Они сводят информационную безопасность в основном к деятельности по защите свойств информации и информационной инфраструктуры техническими и организационными мерами, основываясь на положениях государственных стандартов.

Необходимо выделить и определение понятия информационной безопасности не через состояние защищенности национальных интересов, а через возможность и способность субъектов правоотношений обеспечивать, защищать и развивать информационную сферу.

Различные научные подходы к понятию «информационная безопасность»: от широкого – «состояние защищенности национальных интересов в информационной сфере от внутренних и внешних угроз» (включающего в себя огромное количество направлений деятельности, от противоборства в информационных войнах до защиты персональных данных отдельного гражданина) до узкого – «деятельность по защите свойств информации» – и отсутствие ее закрепления в федеральных нормативно- правовых актах затрудняют научное осмысление таких важных составляющих элементов информационной безопасности, как ее структура и система .

Очевидна необходимость разграничения понятий «информационная безопасность Российской Федерации», «безопасность информационной сферы», «защита информации и информационной структуры».

Современные глобальные тенденции общественного развития можно охарактеризовать такими понятиями и терминами как: постиндустриальное общество, постэкономическое общество, общество знаний, информационное общество, общество потребления, новая экономика, сервисная экономика, инновационная экономика и некоторыми другими, им подобными.

Начиная со 50-х гг. XX в. в развитых странах происходит смена одной стадии исторического развития на другую, постепенный переход от индустриального к постиндустриальному обществу.[5]

В конце 60-70-х гг. XX в. было предложено множество различных концепций «постиндустриального общества». В соответствии с данными концепциями, смена различных технологических эпох, отраслевое и профессиональное разделение труда рассматривается в качестве основы поступательного развития общества. Ведущая роль в постиндустриальном обществе отводится сфере услуг, науке и образованию.

Постиндустриальное общество прежде всего характеризуется тем, что когда человечество достигло определенного экономического благополучия, на первый план выступили и приобрели особое значение не экономические права и свободы, а нематериальные блага, направленные на свободное и полное развитие личности.

- 1. Концепции определяющие природу информационной безопасности

Исследователи выделяют ряд концепций, определяющих природу информации.

Так, первая концепция называется лингвистическая. Она представляет собой толкование информации с помощью использования языковедческих традиций. Так, например, толковый словарь Д.Н. Ушакова дает следующее определение понятию «информация»:

«1) Действие по глаголу информировать;

2) Сообщение, осведомляющее о положении дел или о чьей- нибудь деятельности, сведения о чем-нибудь»[6]. Однако лингвистическое толкование дает только смысловое (т.е. семантическое) значение употребляемого слова.

Вторая концепция нашла своё отражение в физико-математических науках, согласно данной концепции информация понимается в строго научном значении этого понятия. У каждого исследователя свой взгляд на природу информации, эти различия стоит рассматривать не как противоречия, а как разнообразие самой природы информации, что лишний раз подчеркивает актуальность и сложность данной проблемы.

Третья концепция определения природы информации – обществоведческая (социальная) – связана с философским и социальным восприятием этого феномена. Для сторонников данной концепции особый интерес представляют социальные

аспекты информации. Исследования и открытия в этой области привели ряд исследователей к умозаключению, согласно которому природа информации находится в плоскости теории отражения и информационного взаимодействия материальных и нематериальных объектов.[7]

Анализ действующего законодательства показывает, что термин «информация» встречается в большом количестве нормативно-правовых актов, которые относятся к различным отраслям права либо имеют комплексный характер.

В современном мире можно выделить несколько отличающихся друг от друга подходов к обеспечению информационной безопасности. Приоритетным направлением первого подхода является обеспечение информационной открытости, а направлением второго – дозирование информации, обеспечение контроля за доступом к ней.

Раньше в нашей стране проблема правового обеспечения информационной безопасности не только не выдвигалась, но фактически полностью игнорировалась. В настоящее время возрастает роль и значение информационной безопасности в рамках обеспечения национальной безопасности Российской Федерации по следующим основаниям.

Во-первых, одной из главных причиной необходимости поддержания на высоком уровне информационной безопасности является развитие информатизации общества. Исследования показывают, что развитие окружающей информационной среды оказывает значительное воздействие на общественный прогресс и развитие каждого человека. Поэтому, информационная среда нуждается в надежной защите, в том числе правовой.

Во-вторых, в условиях глобализации роль информации возрастает. Она вполне обоснованно может считаться объектом и продуктом труда, одним из основных богатств страны, а также стратегическим национальным ресурсом.

Также нельзя не учесть тот факт, что между научно-техническим прогрессом и информационной безопасностью личности, общества и государства прослеживается прямо пропорциональная связь.[8]

По мере развития науки и техники возрастает роль и значение информационной безопасности.

Многие сферы жизнедеятельности человека, общества и государства трудно представить без последних достижений научно-технического прогресса, которые за последние годы проникли в них настолько, что сделали их зависимыми.

Возросшая роль информации в XXI в., который называют веком информационным, как никогда актуализирует вопрос об обеспечении информационной безопасности. Помимо организационно-технической составляющей обеспечения информационной безопасности значительную роль в этом механизме должно выполнять и право.

Благодаря развитию телекоммуникации появляются новые возможности, способствующие формированию и развитию мирового информационного общества, в котором не только различные ведомства, организации, предприятия и фирмы владеют и пользуются персональным компьютером, подключенным к трансграничным информационным сетям, но и практически каждая семья имеет в собственности это техническое устройство.[9]

Развитие техники способствует появлению новых форм, трансформации существующих видов деятельности с использованием информационных сетей: работа, развлечения, торговля, воспитание, образование и другое. В настоящее время каждый член общества имеет возможность в свободном доступе своевременно получать достоверную информацию, независимо от того, в какой точке географического пространства он находится, также сегодня представляется возможность свободное общение членов общества друг с другом, находясь в различных местностях.

В процессе коммуникации происходит установление связи между различными социальными системами. Поэтому коммуникация является главным инструментом формирования информационного общества. В свою очередь средства массовой информации и Интернет являются проводником реализации политики государства в информационной сфере. Транслируемую с их помощью информацию можно рассматривать как средство манипуляции сознанием людей. При помощи такой манипуляции нередко достигаются политические, коммерческие и другие цели.

В современном мировом сообществе одним из решающих факторов контроля над решением любых проблем является обладание информацией. Именно поэтому изречение Уинстона Черчилля «Кто владеет информацией, тот владеет миром» получило распространение в широких массах населения и является актуальным в свете становления и развития информационного общества.[10]

Обладание информацией позволяет повысить уровень развития различных сфер деятельности государства в целом и отдельно взятого предприятия в частности, что в конечном счете будет способствовать достижению значительных успехов в экономике, бизнесе и финансах. Однако, на субъектов, обладающих ценной информацией, возлагается высокая ответственность за её сохранность и защиту от возможного воздействия различных факторов и событий.

Информация может способствовать возникновению крупномасштабных аварий, разжиганию военных конфликтов, а также дезорганизации государственного управления, финансовой системы и работы научных центров.

Нормативные правовые акты, регулирующие правовые отношения, возникающие в информационной сфере, находятся в хаотичном состоянии и относятся к разным отраслям права. Исследования нормативно-правовой базы, регулирующей информационную сферу, показывают, что нередко прослеживается дублирование правовых норм, а порой и их противоречивость. Эти недостатки препятствуют правильному толкованию и применению правовых норм. В связи с этим, законодательство в информационной сфере нуждается в совершенствовании и прогрессивном развитии.

Ряд исследователей видят разрешение данной проблемы в необходимости систематизации и кодификации информационного законодательства, они объясняют это тем, что систематизация будет способствовать исключению субъективного понимания существующей нормативно-правовой базы в информационной сфере. При этом кодификация будет способствовать:

1) обеспечению единообразного, системного и обоснованного регулирования информационной сферы;

2) приближению регулирования информационных отношений в законодательстве Российской Федерации к международной практике.[11]

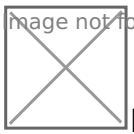
То есть, информация и информационные технологии определяют основные пути и направления развития общества и государства, а также коренным образом влияют на формирование человека как личности, оказывают решающее воздействие на определение его роли и места в обществе.

Таким образом, доктрина информационной безопасности выступает в качестве одного из основных элементов по обеспечению жизненно важных интересов Российской Федерации, так как угрозы национальной безопасности страны во всех

сферах деятельности государства все больше осуществляются через информационную среду.

Глава 2. Разработка информационной системы безопасности банкомата

2.1 Физическая (аппаратная) структура банкомата



Рассмотрим схему прохождения информации о PIN клиента между банкоматом, банком-эквайером (которому принадлежит банкомат) и банком-эмитентом (который выпустил карту клиента) (рис. 2).

Рис. 2. Схема прохождения информации о PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

Пусть клиент Банка 2 (Эмитента) обратился к банкомату Банка 1 (Эквайера). При этом в сети банкоматов происходят следующие действия.[12]

1. Считывающее устройство банкомата считывает информацию, записанную на банковской карте, предъявленной клиентом, и затем банкомат определяет, имеет ли этот клиент счет в Банке 1 - Эквайере.[13]

2. Если клиент не имеет счета в Банке 1, транзакция направляется в сетевой маршрутизатор, который, используя идентификационный номер Банка 2 - Эмитента BIN (Bank Identification Number), направляет эту транзакцию на главный компьютер Банка 2 или производит проверку PIN для Банка 2.

3. Если проверка PIN производится на главном компьютере Банка 2, то этот компьютер получает полную информацию о транзакции и проверяет достоверность PIN.

4. Независимо от результата проверки компьютер Банка 2 пересылает сообщение с этим результатом через сетевой маршрутизатор компьютеру Банка 1.

Как следует из примера, к банку-эмитенту предъявляются следующие требования:

- выпускаемые им карты должны восприниматься всеми банкоматами сети;[14]

- банк-эмитент должен обладать технологией проверки PIN собственных клиентов.

К банку-эквайеру предъявляются другие требования:

- в банкомате или главном компьютере банка должна быть реализована проверка принадлежности транзакции;[15]

- если нет возможности проверить правильность чужого PIN, банк-эквайер должен передать данные о транзакции на сетевой маршрутизатор.

Для защиты взаимодействия компьютеров банков друг с другом и с банкоматами должно применяться оконечное (абонентское) шифрование информации, передаваемой по линиям связи. Обычно используется следующий подход: вся сеть банкоматов разбивается на зоны, и в каждой из них используется свой главный зональный управляющий ключ ZCMK (Zone Control Master Key). Ключ ZCMK предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ ZCMK индивидуален для всех участников сети. Обычно он генерируется случайным образом маршрутизатором и передается неэлектронным способом в банк. Раскрытие ключа ZCMK приведет к раскрытию всех PIN, которые передаются между маршрутизатором и главным компьютером банка

Для шифрования информации, поступающей от главного компьютера банка-эмитента на маршрутизатор, используется рабочий ключ эмитента IWK (Issuer Working Key). Его сообщает главному компьютеру банка-эмитента маршрутизатор в зашифрованном на уникальном ZCMK виде. Ключ IWK может меняться по запросу пользователя в процессе работы.

Аналогичный по назначению ключ для обмена между банком-эквайером и маршрутизатором называется рабочим ключом эквайера AWK (Acquirer Working Key). Для шифрования информации при передаче от банкомата к главному компьютеру банка-эквайера используется связной ключ эквайера ACK (Acquirer Communication Key).

При рассмотрении функционирования системы защиты введены следующие обозначения:[16]

EY (X) - шифрование сообщения X по алгоритму DES с использованием ключа Y;

DY (X) - расшифрование сообщения X по алгоритму DES с использованием ключа Y;

PBL (PIN Block Local) - локальный блок PIN, полученный из введенного клиентом PIN, дополненного до восьми символов, и представленный во внутреннем формате банкомата;

PBN (PIN Block Network) - сетевой блок PIN, полученный из введенного клиентом PIN, дополненного до восьми символов, и представленный в виде, готовом для передачи в сети.

1. Клиент предъявил банкомату Банка 1 банковскую карту и ввел с клавиатуры свой PIN. Банкомат формирует PBL, шифрует его с использованием АСК, т.е. вычисляет криптограмму ЕАск(PBL), и отправляет ее на главный компьютер Банка 1.

2. На главном компьютере Банка 1 блок PBL расшифровывается и преобразуется в блок PBN, затем блок PBN шифруется с использованием AWK и отсылается в Сетевой маршрутизатор. Процесс преобразования

EACK (PBL) -> EAWK (PBN)

называют трансляцией блока PIN с ключа ACK на ключ AWK. Основное назначение этого процесса – смена ключа шифрования.

3. Если PIN проверяется на Сетевом маршрутизаторе, после получения криптограммы eawk(pbn) производится ее расшифрование, а затем выделение PIN с помощью преобразований

d AWK (e awk (pbn)) = PBN -> PIN.

Если PIN проверяется Банком 2, принятая криптограмма транслируется с ключа AWK на ключ IWK (оба ключа хранятся на Сетевом маршрутизаторе):

EAWK (PBN) -> EIWK(PBN).

Затем криптограмма EIWK(PBN) отправляется в Банк 2.

4. Поступившая в Банк 2 криптограмма EIWK(PBN) преобразуется в зависимости от используемого способа проверки либо в открытый PIN:

DIWK (EIWK (PBN)) = PBN->PIN,

либо в PIN в форме блока PBL, зашифрованного на ключе базы данных DBK:

E IWK (PBN) -> EDBK (PBL).

5. После любого из этих преобразований осуществляется поиск принятого PIN в базе данных существующих PIN.

6. В результате выполненной проверки введенный клиентом PIN либо принимается, либо отвергается. Вне зависимости от результата проверки главный компьютер Банка 2 пересылает сообщение с результатом через Сетевой маршрутизатор на компьютер Банка 1, а тот оповещает банкомат о результатах решения.[17]

Рассмотренная схема обеспечения безопасности взаимодействия компьютеров в сети базируется на симметричном алгоритме шифрования DES. Поэтому на распространение ключа ZCMK налагаются жесткие ограничения. Применение асимметричной системы шифрования с открытым ключом позволяет несколько упростить ключевую систему и соответственно взаимодействие между банкоматами и главными компьютерами банков.

В неразделяемой сети банкоматов достаточно использовать на всех банкоматах одинаковый открытый ключ, а на главном компьютере банка - закрытый ключ. Это позволяет шифровать запрос и подтверждающее сообщение из банка, так как обеспечение конфиденциальности ответного сообщения необязательно.

Проблема защиты запроса от активных атак (изменения или введения ложного запроса) может быть решена в случае неразделяемой сети использованием пароля для идентификации банкоматов.

2.2 Программная структура: анализ и выбор состава и структуры общего и специального мат. обеспечения объекта проектирования

Миллионы людей во всем мире пользуются банковскими карточками. Рост электронной коммерции, удобство оплаты без использования наличных денег, безопасность транзакций, практичность неизменно ведут к росту использования платежных карточек. По итогам на 2005 г. в РФ было выдано более 54 млн. банковских карт, и эта цифра увеличивается примерно в 1.5 раза в год.

Необходимость защиты транзакций POS-терминалов и банкоматов продиктована, прежде всего, требованиями компаний платежных систем (Visa, MasterCard, American Express и пр.), а также многочисленными нормативными актами по конфиденциальности и защите информации.

Производители банковского оборудования – POS-терминалов и банкоматов – активно продвигают на рынок модели оборудования, способные подключаться к локальным сетям, а также сетям GPRS, Bluetooth и пр.

Подключение POS-терминала или банкомата к локальной сети заставляет обеспечить не только своевременную и надежную обработку транзакции, но и ее конфиденциальность. Большинство нового оборудования поддерживает стандарт SSL (Secure Sockets Layer), что позволяет шифровать конфиденциальную информацию между POS-терминалом или банкоматом, и системой, обрабатывающей транзакции (HOST). Очевидной также становится более низкая стоимость подключения большого числа банкоматов или POS-терминалов к локальной сети клиентов (филиалов, торговых точек), по сравнению со стоимостью выделенных телефонных линий, модемных пулов и соответствующего оборудования. Архитектура SSL является общепризнанным стандартом безопасности и позволяет заказчику использовать наилучшие решения от разных производителей[18].

Компания Radware, совместно с партнерами-производителями оборудования POS-терминалов, а также с ведущими интеграторами в этой области, предлагает эффективное и экономичное решение для обеспечения безопасности транзакций.

Решение предлагается с использованием платформы ускорения транзакций Radware AppXcel.

Для проведения онлайновой транзакции, терминал открывает TCP-соединение через локальную сеть (возможны варианты внедрения GPRS, Bluetooth и пр.) на устройство AppXcel. Далее терминал устанавливает SSL-сессию и посылает зашифрованные данные транзакции. Radware AppXcel открывает TCP-соединение на хост и посылает расшифрованные данные, а также шифрует и отправляет на терминал ответы хоста.[19]

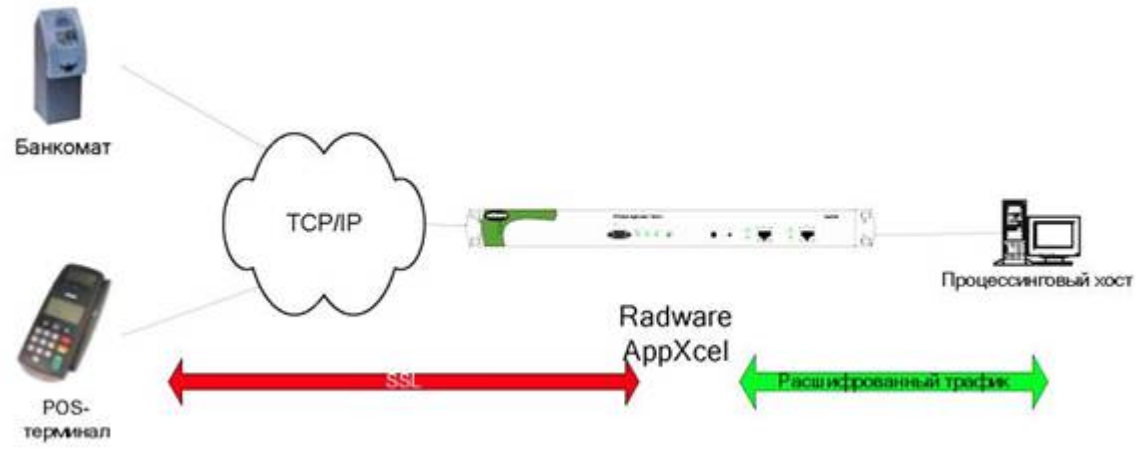


Рис. 3 Установка с использованием резервного устройства AppXcel для обеспечения отказоустойчивости

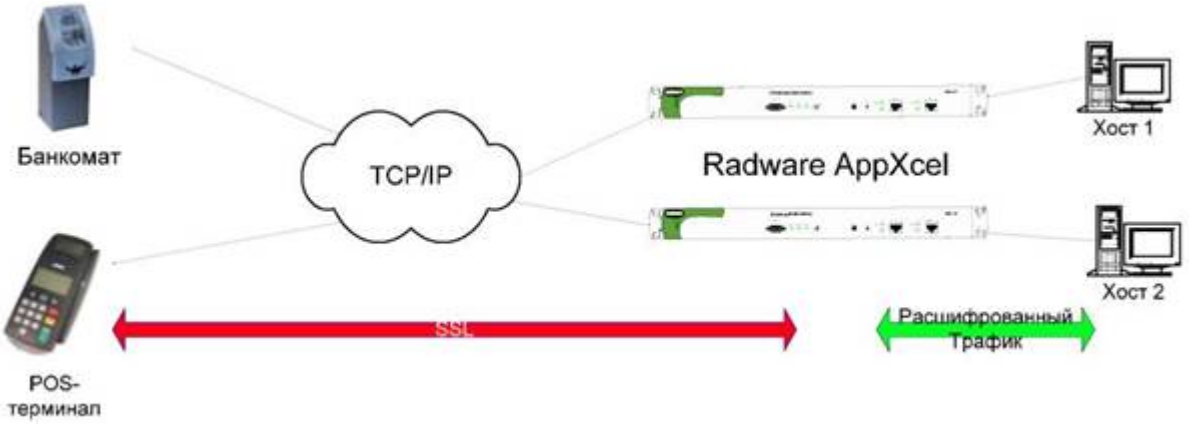


Рис.4. Установка с использованием резервного устройства AppXcel для обеспечения отказоустойчивости

В данном варианте установки в POS-терминалах и банкоматах устанавливаются учетные записи двух хостов. При отказе одного из них, банкомат или терминал самостоятельно направляют запрос на резервный хост, что позволяет достичь высокого уровня отказоустойчивости.

Высокопроизводительное решение, с возможностью масштабирования и обеспечением отказоустойчивости всех компонентов.[20]

При высоком уровне транзакций возможна установка балансировщика нагрузки Radware AppDirector для обеспечения равномерного распределения транзакций, мониторинга состояния сетевых элементов, масштабирования и отказоустойчивости. При необходимости увеличения масштабов обработки транзакций требуется лишь подключить дополнительные устройства AppXcel, не

меняя архитектуры решения. Отказоустойчивость решения обеспечена резервированием балансировщика нагрузки AppDirector и устройств AppXcel.

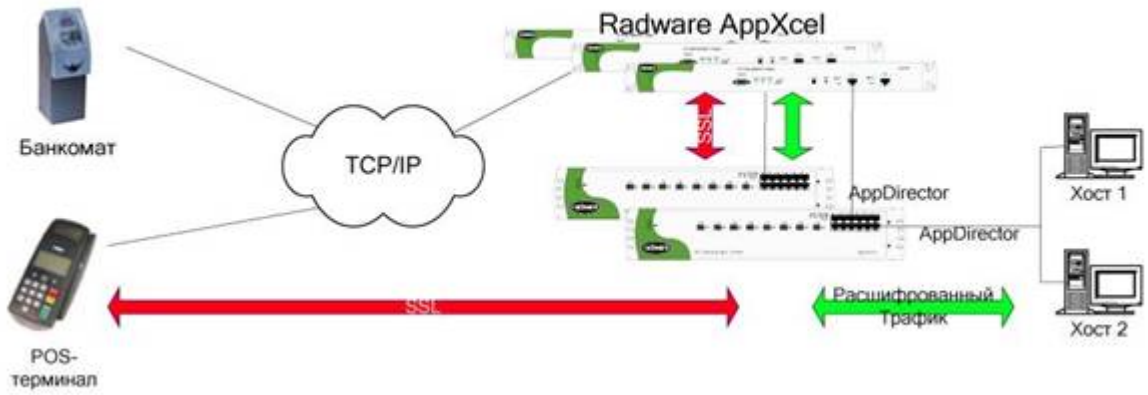


Рис.5. Установка с использованием резервного устройства AppXcel с балансировщиком нагрузки Radware AppDirector

2.3 Выбор показателей, способов оценки и оценка эффективности принятых проектных решений

Функция AppXcel	Выгоды IT	Преимущества APSolute	Бизнес-выгоды

Бизнес - выгоды	• Консолидация или снижение операционных и эксплутационных затрат на 40% • Обеспечение непрерывности служб SSL и выполнения транзакций	• До 16,000 транзакций в секунду и 150,000 одновременных соединений • Кластеризация (соединение и интеграция нескольких серверов с целью обеспечения высокого коэффициента готовности и масштабируемости системы) для резервирования и масштабируемая работа с более чем 35,000 терминалами. • Поддерживаемые алгоритмы: DES, 3DES, DH, DSS, MD5, RC2,RC4, RSA,SHA-1 • Поддерживаемые протоколы: SSLv2, SSLv3, TLS, FTPS, SMTPS, POP3S, IMAPS, LDAPS, SIP/TLS. • Шифрование: до 168 бит • Длина ключа: 512-20468 бит • Поддержка всех коммерческих web-серверов • Поддержка	• Снижение информационно - технологических затрат: – Большая производительность меньшего количества серверов – Облегченное управление безопасностью информации и SSL • Увеличение продуктивности при ускорении работы бизнес-приложений.

Централизованное управление приложениями и SSL	• Централизованное управление и ключевая защита от копирования: снижает сложность и стоимость управления инфраструктурой SSLсерверов. • Снижение эксплуатационных затрат при установке и управлении сертификатами на каждом сервере. • Упрощение обслуживания и диагностики. • Снижение стоимости внедрения федерального стандарта обработки информации до 50% • Централизованный мониторинг работы SSL	• APSolute Insite – сетевая конфигурация на основе пользовательского графического интерфейса, консоль мониторинга и управления • Протокол SNMP v1, v2, v3 • Также поддерживает: - Безопасное внутриполосное Web-управление и интерфейс командной строки (Telnet или SSH) - Внеполосный интерфейс командной строки RS-232 • Поддержка отчетов по каналам SNMP, системные записи и электронные сообщения • Плагин (подключаемая программа) HP OpenView • Многоаппаратная передача полномочий в сети • Подтверждено FIPS

2.4 Меры защиты банкоматов

Одним из ведущих продуктов защиты банкоматов является Safe'n'Sec TPSecure. Защита банкоматов с помощью Safe'n'Sec TPSecure осуществляется в соответствии с политиками контроля активности приложений. Продукт контролирует каждое действие в процессе работы системы, блокирует все подозрительные действия и разрешает исполняться только доверенным процессам из так называемого «белого» списка (списка доверенных процессов). Именно такой подход, пожалуй, наиболее эффективен для обеспечения защиты банкоматов и POS-терминалов, так как набор активных процессов в них очень стабилен. При установленном Safe'n'Sec TPSecure запуск неопознанных приложений невозможен до тех пор, пока пользователь с соответствующими правами не укажет степень доверия к этому приложению.[21]

На самом деле Safe'n'Sec TPSecure - это не просто блокирование по белым спискам. Он основан на технологии V.I.P.O. (Valid Inside Permitted Operations), которая объединяет в себе адаптивное профилирование, выполнение приложений в защищенной среде (sandbox - «песочница») и подсистему поведенческого анализа.

Рис.6.Уровни защиты Safe’n’Sec

Технология V.I.P.O. основана на перехвате вызовов системных функций на уровне ядра операционной системы (Ring 0) и загружается раньше всех остальных приложений. Она позволяет идентифицировать, анализировать и, при необходимости, блокировать доступ к файловой системе, объектам системного реестра, к запуску приложений и к другим операциям, способным воздействовать на целостность защищаемых приложений. Таким образом, технология V.I.P.O.

создает защиту ядра операционной системы для предотвращения запуска любого нежелательного кода.[22]

После установки Safe'n'Sec TPSecure и его первоначальной настройки оперативное администрирование больше не потребуется, так как решение не нуждается в постоянном обновлении. Safe'n'Sec TPSecure будет полностью автоматически блокировать все несанкционированные действия, поскольку для восстановления оборудования и возобновления его работы не потребуется перезагрузка системы.

Выполнения несанкционированного кода, пытающегося внедриться в операционную систему, предотвращается при помощи изолированной виртуальной среды - «песочницы». В ней код может выполняться безопасно для вычислительной системы, не воздействуя на другие ее части. На практике это означает, что вредоносная программа не может получить доступ к операционной системе, разрешенным приложениям или буферу обмена данными для внедрения перехватчиков, клавиатурных шпионов и других нежелательных программ. Это также означает невозможность изменить код и данные, принадлежащие другим процессам, а также несанкционированно модифицировать исполняемые файлы.[23]

2.5 Функциональные возможности Safe'n'Sec TPSecure

Блокировка любой возможности несанкционированного подключения и внедрения всякого рода ПО со стороны обслуживающего банкоматы персонала.

Защита доступа к критически важным данным (владельцы карт, PIN-коды, пароли).

Контроль всех событий в сети, событий в банкоматах и генерирует консолидированный аналитический отчет с широкими возможностями фильтрации с целью ретроспективного анализа и расследования конкретного инцидента вторжения вредоносного кода.

Мобильная консоль централизованного управления (позволяет существенно снизить временные затраты на развертывание системы безопасности).

Автономная работы (без связи с сервером управления).

Важно отметить, что настройка Safe'n'Sec TPSecure осуществляется специалистами S.N. Safe&Software под запросы и нужды конкретного заказчика. При этом общая стоимость владения комплексным продуктом остается для клиентов на уровне стандартных продуктов.

Заключение

В связи с возрастанием роли информации XXI в. называют веком информационным. В условиях информатизации общества в качестве одной из основных задач выделяют правовое регулирование информационной безопасности.

Состав угроз информационной безопасности всегда играла в жизни человека очень большую роль, но с середины 20-го века в результате социального прогресса и прорыва в развитии науки и техники роль информации неизмеримо возросла. Теперь, с усовершенствованием информационных технологий, можно совершить ту или иную платежную операцию в любом месте города, страны, так как в современном обществе банкоматы находятся в каждом магазине, торговых зданиях, учреждениях, организациях и даже офисах.

В данной курсовой работе меры защиты информации при платежных операциях осуществлялись через переход от закрытых систем обработки транзакций к открытым системам. Это позволит клиенту с легкостью найти нужную ему информацию по платежным операциям. А также вся установка и эксплуатация этой системы обходится с минимальными расходами. Усовершенствование транзакций для автоматических терминалов смогут защитить банкоматы от известных и неизвестных угроз.

Список использованной литературы

Нормативные правовые акты

1. Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)»: постановление Правительства Российской Федерации от 15.04.2014 № 313: офиц. текст по состоянию на 21.02.2015 // Собрание законодательства Российской Федерации. – 05.05.2014. – № 18 (часть II). – Ст. 2159.

Монографии и учебные пособия

2.Бодров, О.А. Предметно-ориентированные экономические информационные системы: Учебник для вузов / О.А. Бодров. - М.: Гор. линия-Телеком, 2013. - 244 с.

3. Варфоломеева, А.О. Информационные системы предприятия: Учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. - М.: НИЦ ИНФРА-М, 2013. - 283 с.

4.Вдовин, В.М. Предметно-ориентированные экономические информационные системы: Учебное пособие / В.М. Вдовин. - М.: Дашков и К, 2013. - 388 с.

5. Демьянец М. В. Предпринимательская деятельность в сети Интернет: Монография / М. В. Демьянец, В. М. Елин, А. К. Жарова. – М. : ЮРКОМПАНИ. – 2014. – 440 с.

6. Жеребин В. М. Социальные аспекты информатизации: Монография / В. М. Жеребин. – М. : Экономическое образование. – 2013. – 212 с.

7. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – СПб. : СПбНИУИТМО. – 2014. – 173 с.

8. Санжаревский И. И. Политическая наука: словарь-справочник. Изд. 6-е, испр. и доп. / И. И. Санжаревский. – Тамбов. – 2014. – 750 с.

9. Снетков В. Н. Власть в обществе и информационная политика / В. Н. Снетков, А. В. Пономаренко. – СПб. : Изд-во СПбГПУ. – 2001. – 247 с.

10.Мезенцев, К.Н. Автоматизированные информационные системы: Учебник для студентов учреждений среднего профессионального образования / К.Н. Мезенцев. - М.: ИЦ Академия, 2013. - 176 с.

11.*Терещенко Л. К.* Модернизация информационных отношений и информационного законодательства: Монография / Л. К. Терещенко. – М. : ИНФРА-М. – 2013. – 227 с.

12.Уткин, В.Б. Информационные системы в экономике: Учебник для студентов высших учебных заведений / В.Б. Уткин, К.В. Балдин. - М.: ИЦ Академия, 2012. - 288 с.

Научные статьи

13. Вербицкая Т. Суды о национальной безопасности / Т. Вербицкая // ЭЖ-Юрист. – 2014. – № 13. – С. 1-6.

14. Емелькина И. В. Основные характеристики российского менталитета в условиях информационного общества / И. В. Емелькина // Информационное право. – 2011. – №

1. – С. 27-29.

15.*Мигачев Ю. И.* Правовые основы национальной безопасности (административные и информационные аспекты) / Ю. И. Мигачев, Н. А. Молчанов // Административное право и процесс. – 2014. – № 1. – С. 46-49.

16.Михайлёнок О. М. Политические аспекты информационной безопасности личности / О. М. Михайлёнок // Власть. – 2010. – № 12. – С. 64-70.

17.Номоконов В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55.

18.Попов В. В. Информация как фактор воздействия на политическую жизнь общества (социокультурный аспект) / В. В. Попов // Вопросы безопасности. – 2014. – № 6. – С. 68-97.

19.Смирнов А. А. К вопросу о понятии, объекте и содержании информационно-психологической безопасности / А. А. Смирнов // Административное право и процесс. – 2013. – № 1. – С. 34-39

20.Снетков В. Н. Обеспечение информационной безопасности в условиях гражданского общества / В. Н. Снетков // Проблемы права в современной России : сборник статей международной межвузовской научно- практической конференции. – СПб. : Изд-во Политехн. ун-та. – 2012. – С. 198-202

21.*Холопова Е. Н.* Информационная безопасность пограничных органов на современном этапе: понятие, структура / Е. Н. Холопова, А. С. Бойцов // Информационное право. – 2014 – № 5. – С. 4-9.

22.Ясенев, В.Н. Информационные системы и технологии в экономике.: Учебное пособие для студентов вузов / В.Н. Ясенев. - М.: ЮНИТИ-ДАНА, 2012. - 560 с.

Электронные ресурсы

23.Официальный сайт Совета Безопасности Российской Федерации // URL : http://www.scrf.gov.ru/news/19/874.html (дата обращения 05.04.2015).

1. Бодров, О.А. Предметно-ориентированные экономические информационные системы: Учебник для вузов / О.А. Бодров. - М.: Гор. линия-Телеком, 2013. - 244

с. ↑

2. Демьянец М. В. Предпринимательская деятельность в сети Интернет: Монография / М. В. Демьянец, В. М. Елин, А. К. Жарова. – М. : ЮРКОМПАНИ. – 2014. – 440 с. ↑

3. Варфоломеева, А.О. Информационные системы предприятия: Учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. - М.: НИЦ ИНФРА-М, 2013. - 283 с. ↑

4. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – СПб. : СПбНИУИТМО. – 2014. – 173 с. ↑

5. Вдовин, В.М. Предметно-ориентированные экономические информационные системы: Учебное пособие / В.М. Вдовин. - М.: Дашков и К, 2013. - 388 с. ↑

6. Санжаревский И. И. Политическая наука: словарь-справочник. Изд. 6-е, испр. и доп. / И. И. Санжаревский. – Тамбов. – 2014. – 750 с. ↑

7. Бодров, О.А. Предметно-ориентированные экономические информационные системы: Учебник для вузов / О.А. Бодров. - М.: Гор. линия-Телеком, 2013. - 244 с. ↑

8. Жеребин В. М. Социальные аспекты информатизации: Монография / В. М. Жеребин. – М. : Экономическое образование. – 2013. – 212 с. ↑

9. Мезенцев, К.Н. Автоматизированные информационные системы: Учебник для студентов учреждений среднего профессионального образования / К.Н. Мезенцев. - М.: ИЦ Академия, 2013. - 176 с. ↑

10. Снетков В. Н. Власть в обществе и информационная политика / В. Н. Снетков, А. В. Пономаренко. – СПб. : Изд-во СПбГПУ. – 2001. – 247 с. ↑

11. Терещенко Л. К. Модернизация информационных отношений и информационного законодательства: Монография / Л. К. Терещенко. – М. : ИНФРА-М. – 2013. – 227 с. ↑

12. Официальный сайт Совета Безопасности Российской Федерации // URL : http://www.scrf.gov.ru/news/19/874.html (дата обращения 05.04.2015). ↑

13. Уткин, В.Б. Информационные системы в экономике: Учебник для студентов высших учебных заведений / В.Б. Уткин, К.В. Балдин. - М.: ИЦ Академия, 2012. - 288 с. ↑

14. Ясенев, В.Н. Информационные системы и технологии в экономике.: Учебное пособие для студентов вузов / В.Н. Ясенев. - М.: ЮНИТИ-ДАНА, 2012. - 560 с. ↑

15. Михайлёнок О. М. Политические аспекты информационной безопасности личности / О. М. Михайлёнок // Власть. – 2010. – № 12. – С. 64-70. ↑

16. Вербицкая Т. Суды о национальной безопасности / Т. Вербицкая // ЭЖ-Юрист. – 2014. – № 13. – С. 1-6. ↑

17. Номоконов В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55. ↑

18. Емелькина И. В. Основные характеристики российского менталитета в условиях информационного общества / И. В. Емелькина // Информационное право. – 2011. – № 1. – С. 27-29. ↑

19. Смирнов А. А. К вопросу о понятии, объекте и содержании информационно-психологической безопасности / А. А. Смирнов // Административное право и процесс. – 2013. – № 1. – С. 34-39 ↑

20. Мигачев Ю. И. Правовые основы национальной безопасности (административные и информационные аспекты) / Ю. И. Мигачев, Н. А.

Молчанов // Административное право и процесс. – 2014. – № 1. – С. 46-49. ↑

21. Попов В. В. Информация как фактор воздействия на политическую жизнь общества (социокультурный аспект) / В. В. Попов // Вопросы безопасности. – 2014. – № 6. – С. 68-97. ↑

22. Снетков В. Н. Обеспечение информационной безопасности в условиях гражданского общества / В. Н. Снетков // Проблемы права в современной России : сборник статей международной межвузовской научно- практической конференции. – СПб. : Изд-во Политехн. ун-та. – 2012. – С. 198-202 ↑

23. Холопова Е. Н. Информационная безопасность пограничных органов на современном этапе: понятие, структура / Е. Н. Холопова, А. С. Бойцов // Информационное право. – 2014 – № 5. – С. 4-9. ↑