План

1. Введение
2. Основная часть
   1. Новые направления, стимулируемые банковскими приложениями
   2. Современные средства защиты
   3. Банк защищается от клерков
   4. Система «свой-чужой» для банка и клиента
   5. Криптография — дело федеральной безопасности
   6. Рост спроса на биометрию — десятки процентов в год
   7. Обеспечиваемая шифром степень защиты
   8. Основные цели информационной безопасности
3. Заключение
4. Список литературы
5. Введение

В своей работе я хочу рассмотреть направления защиты информации, стимулируемые банковскими приложениями. Также хочу рассказать что же такое криптография, рассмотреть средства защиты информации и основные цели информационной безопасности.

1. Основная часть

2.1. Новые направления, стимулируемые банковскими приложениями

Существуют криптографические схемы (такие как криптосистемы, схемы электронной подписи и т. п.) универсального назначения. По отношению ко всем этим схемам защита банковской информации - всего лишь одна из возможных областей применения. В то же время в теоретической криптографии имеются два направления исследований, разрабатываемых специально и исключительно для банковских приложений. Сюда относятся так называемые банковские криптографические протоколы и криптографическое обеспечение банковских карточек. В современном понимании банковская карточка - это интеллектуальная карточка с соответствующей «начинкой». Криптографическая часть подобной начинки может включать в себя как специфические для банков компоненты, так и криптоалгоритмы, реализующие схемы аутентификации, электронной подписи и т. п.

Криптография - это искусство скрытия информации в последовательности битов от любого несанкционированного доступа. Для достижения этой цели используют шифрование: сообщение с помощью некоторого алгоритма комбинируется с дополнительной секретной информацией (ключом), в результате чего получается криптограмма. Долгое время способы разработки алгоритмов шифрования определялись исключительно хитростью и изобретательностью их авторов. И лишь в ХХ веке этой областью заинтересовались математики, а впоследствии - и физики.

Интеллектуальные карточки - это новое поколение пластиковых карточек, отличающееся от всех предшествующих развитыми возможностями для реализации средств защиты информации. В банковских системах недалекого будущего интеллектуальные карточки, по-видимому, станут основным платежным средством, вытеснив ныне используемые карточки с магнитной полосой. Вместе с тем имеющиеся в интеллектуальных карточках вычислительные возможности еще недостаточны для эффективной реализации сложных криптографических схем. Поэтому проблема компромисса между эффективностью реализации и стойкостью криптографических схем остается достаточно острой для банковских систем, использующих интеллектуальные карточки.

Второе новое направление - это банковские криптографические протоколы, обеспечивающие безопасность систем электронных платежей. Иногда ныне используемые автоматизированные системы банковских расчетов также называют системами электронных платежей. Но на самом деле они представляют собой системы безналичного расчета с использованием современных средств связи. В «настоящих» же системах электронных платежей бумажные деньги полностью заменяются электронными деньгами, которые могут использоваться клиентами для платежей при расчетах не только с банком, но и между собой. Другой отличительной особенностью систем электронных платежей является обеспечение неотслеживаемости действий клиентов. Необходимость обеспечения неотслеживаемости зарубежные специалисты объясняют на примерах подобных следующему. Находящиеся ныне в обращении кредитные карточки полностью идентифицируют их владельцев при каждом платеже. Если клиент использует кредитную карточку для покупки билетов на автобусы, то транспортная компания тем самым имеет возможность отслеживать все его поездки. Разумеется, подобное злоупотребление не выглядит слишком серьезной угрозой, однако обобщение сценария на случай переводов крупных сумм и участия организованной преступности очевидно. Необходимость обезопасить автоматизированные банковские системы от посягательств уголовных элементов хорошо осознана разработчиками. Однако они пытаются обеспечивать безопасность путем шифрования данных, не отдавая себе отчета в том, что здесь речь идет о неотслеживаемости, а вовсе не о конфиденциальности.

Из сказанного выше становится очевидной несостоятельность следующего тезиса противников неотслеживаемости: она (неотслеживаемость) не нужна, поскольку если клиент не доверяет банку, то он никогда не положит в этот банк свои деньги. На самом деле клиент не доверяет персоналу, работающему в банке и третьим лицам, которые могут перехватывать информацию в каналах связи. С другой стороны, всякий банк, который заботится о неотслеживаемости платежей, повышает доверие клиентов к себе.

Индивидуальным платежным средством в системах электронных платежей является электронный бумажник клиента. Электронный бумажник - это карманный вычислитель со встроенным в него защищенным модулем. Бумажник выдается клиенту и используется в системах электронных платежей как электронные бумажники, с одной стороны, обеспечивают неотслеживаемость действий клиента, а с другой - безопасность банка и высокую эффективность системы электронных платежей.[[1]](#footnote-1)1

* 1. Современные средства защиты

Цена перестала быть критерием выбора средств защиты информации для банков. Рынок программных и аппаратных средств защиты банковской информации стремительно растет — эксперты называют и десятки, и сотни процентов роста объемов в год по разным направлениям. Да так ли важны точные оценки, если «паранойя» в банках развивается по нарастающей: расширяя бизнес, банки понесли первые потери, оценили угрозы и теперь защищаются от клерков, шпионов, мошенников.

Рынок растет и будет расти. Большинство экспертов остерегаются давать количественные характеристики нынешнего состояния рынка систем криптографической защиты информации в целом и прогнозировать темпы его роста. Но наглядное представление о динамике роста могут дать цифры по отдельным сегментам. Генеральный директор компании Aladdin Сергей Груздев приводит следующие данные: «В сегменте рынка, на котором работает наша компания, спрос на средства усиленной аутентификации как коммерческими банками, так и организациями ЦБ РФ вырос примерно в три раза по сравнению с показателями прошлого года. На простейшие идентификаторы, такие как «таблетки», типа iButton, спрос также вырос и составил порядка 40%».

Разброс же цен на отдельные продукты очень велик — от 5 долларов за лицензию и до нескольких сотен долларов за клиентское место. В некоторых случаях стоимость может возрастать до нескольких тысяч долларов, если речь идет об аппаратуре.

Что касается качественных характеристик развития рынка, то здесь оценки наблюдателей довольно сильно разнятся. Одни считают, что рынок переживает качественные перемены спроса. «В целом сегодня мы наблюдаем активный переход от использования дискет, «таблеток» и иных простых идентификаторов к применению более надежных и защищенных носителей, таких как смарт-карты и USB-ключи с функциональностью смарт-карт. В основном ставка делается на сертифицированные носители и использование их для хранения цифровых сертификатов и применения российской криптографии», — рассказывает С. Груздев (Aladdin). В связи с этим позитивной тенденцией является то, что сегодня банки делают свой выбор исходя из функциональных возможностей и надежности носителей. Цена перестала быть приоритетным (а зачастую и единственным) критерием выбора, как это было ранее.

Другие эксперты говорят об отсутствии изменений революционного характера, равно как и предпосылок для их возникновения. «Системообразующих изменений не происходит. Появляются новые продукты, выходят новые версии существующих. Но по сути ничего радикально нового мы не наблюдаем. На общем фоне ровного развития рынка заметна, пожалуй, тенденция на удешевление средств защиты информации. Также есть тренд на более глубокую интеграцию СКЗИ и прикладного ПО», — говорит директор департамента систем электронного банковского обслуживания компании R-Style Softlab Виктор Иванов.

Эксперт считает, что можно быть твердо уверенным в росте интереса банков к более совершенным антивирусным средствам защиты и средствам криптозащиты с течением времени. По мере развития филиальной сети у банков появятся новые дополнительные каналы передачи данных, которые в свою очередь потребуют средств защиты. Так что будет расти объем рынка, равно как и качество предлагаемых продуктов.

* 1. Банк защищается от клерков

Сергей Груздев (Aladdin) полагает, что с точки зрения тенденций внутри банка очевидно, что изменилась основная модель угроз безопасности. На первый план выдвигаются продукты, связанные с защитой от инсайдера, то есть собственного сотрудника банка. Мы наблюдаем резкий рост интереса организаций банковской сферы к этой теме. Здесь можно обозначить, по крайней мере, две тенденции: стремительный отказ от малоэффективной парольной защиты (логин-пароль) и переход к единому идентификатору (USB-ключу или смарт-карте) для доступа ко всем приложениям, а также для доступа в помещения (смарт-карта) с возможностью отслеживания по RFID-меткам местонахождения сотрудника. Единая смарт-карта особенно востребована в тех банках, где согласованы действия службы физической безопасности и офицера по информационной безопасности (ИБ).

В том, что внутренние угрозы представляют несравненно большую опасность, нежели внешние, согласны практически все аналитики. Так, по данным заместителя Института банковского дела Ассоциации российских банков (АРБ) Бориса Скородумова, 76% всех преступлений в банке совершается непосредственно его сотрудниками или же с их непосредственным участием. Не случайно краеугольным камнем целостной системы риск-менеджмента является предупреждение и нейтрализация именно операционных рисков.

С уверенностью можно сказать, что катализатором активного распространения единых средств идентификации стало появление универсальных систем управления жизненным циклом электронных ключей (например, Token TMS — Token Management System) и смарт-карт (CMS — Card Management System) в масштабе предприятия. Этот продукт является связующим звеном между пользователями, их средствами аутентификации, security-приложениями и политикой безопасности, принятой в банке. Такие системы обеспечивают «прозрачность» управления и переводят административный контроль банковской информационной инфраструктуры на качественно новый уровень. Кто-то говорит об установлении, по сути, тотального контроля. Кто-то об упрощении жизни пользователя, поскольку теперь ему не приходится запоминать по 5—7 паролей для доступа к каждому приложению или — что сводит на нет все усилия офицера по ИБ — записывать эти пароли. Но это всего лишь разница оценочных, но не содержательных суждений.

* 1. Система «свой-чужой» для банка и клиента

Востребованность банками тех или иных продуктов жестко детерминируется самим характером угроз. Лавинообразный рост номенклатуры и доли банковских услуг с использованием интернета в «линейке» банковских предложений привел к возникновению новой группы взаимосвязанных преступлений. Ничего более точного для обозначения этого явления, чем калька с английского fishing — «фишинг», — русский язык пока не предложил. Фишингом именуется тип компьютерного мошенничества, основанный на создании поддельных web-ресурсов, позволяющих ввести пользователя в заблуждение (через спам, например, письма с заголовком «Извещение пользователей банковских услуг о переходе на новую систему зачисления платежей») и получить его конфиденциальные данные, как то: пароль, PIN-код и т.п. Причем пользователь, попавший в сети фишера, может наблюдать настоящий адрес банковского сайта в адресной строке браузера, но находиться сам при этом будет на сайте-подделке. Таким образом, продукты, защищающие от перехвата конфиденциальных данных, являются одними из самых востребованных сегодня.

Для того чтобы адекватно оценить масштабы угрозы, имеет смысл обратиться к цифрам, характеризующим динамику роста потока «инфицированных» писем. Согласно данным компании Postini, уже в июле текущего года количество такого рода сообщений перевалило за 19 млн. (из 8 млрд. совокупного числа электронных посланий). Для сравнения, в апреле их было зафиксировано лишь 9,7 млн. То есть за квартал их количество увеличилось без малого на 100%. А сумма ежегодно наносимого ущерба, по исчислениям глобального аналитического центра Gartner, уже с 2003 года зашкаливает за миллиард долларов.

Что может спасти от фишинга? Например, взаимная двухфакторная аутентификация клиента с одной стороны (с использованием отчуждаемого защищенного носителя) и банка — с другой. Используя надежный идентификатор, USB-ключ или смарт-карту, пользователь подключает его и вводит свой PIN-код на странице банка, после чего происходит взаимная аутентификация пользователя и банковского информационного ресурса. Если она прошла успешно, пользователь может быть уверен, что находится именно на этой web-странице именно этого банка и никто не «слушает» его трафик. Двусторонняя аутентификация обеспечивает также и гарантию того, что это именно тот пользователь, за которого он себя выдает, а не злоумышленник, решивший воспользоваться чужим банковским счетом в своих целях.

Топ-менеджмент ряда «прогрессивных» российских банков уже приходит к осознанию того, что использование простейших способов аутентификации, типа «логин-пароль», не обеспечивает нужной степени защиты, и это серьезным образом подрывает доверие к дистанционным технологиям обслуживания клиентов, интернет-банкингу и т.п., что не может не сказываться на репутации банка. О том, насколько узок круг «прогрессивных», можно судить на примере США, где, по данным Gartner, лишь около половины банков располагают продвинутыми технологиями аутентификации.

«Наши заказчики — пионеры внедрения технологий строгой аутентификации — в основном берут все расходы по приобретению более надежных идентификаторов на себя и бесплатно, но в обязательном порядке раздают их своим клиентам, чтобы обезопасить свой бизнес и сохранить репутацию. И это — еще одна тенденция современного банковского бизнеса», — говорит гендиректор Aladdin.

* 1. Криптография — дело федеральной безопасности

Вторая серьезная угроза, актуальная для любого бизнеса, а для банковского — вдвойне, это spyware — программы-шпионы. Этот своего рода злонамеренный код пишется специально для того, чтобы незаметно для пользователя собирать различную информацию о нем и автоматически отправлять ее своему создателю. «Шпионы» «подсаживаются» на компьютер при посещении пользователем каких-либо web-ресурсов или при открытии им неблагонадежного письма и скачивают любую информацию, представляющую интерес для автора «шпиона».

В настоящее время разработка программ-шпионов для осуществления заказной атаки в отношении отдельного банка или конкретного должностного лица, имеющего критически важную информацию, приносит их создателям весьма серьезный доход. Предложение подобных услуг можно встретить в сети интернет. А цена делает их доступными для широкого круга потребителей.

Обезопасить банк от таких атак можно, лишь комплексно подойдя к вопросу контент-безопасности, где речь идет уже не о защите информационных ресурсов банка по внешнему периметру, что очевидно, но о защите внутренних информационных потоков для контролирования каждого пользователя и той информации, которая от него исходит.

Также нельзя обойти вниманием проблему чрезмерной регламентации рынка со стороны государства. Сферу СКЗИ регулируют два ведомства — Гостехкомиссия и ФСБ. Гостехкомисия занимается выдачей лицензий на разработку защищенных средств, в первую очередь аппаратуры. В сфере компетенции ФСБ — сертификация и учет обращения средств шифрования и электронной подписи (средства криптографии). Для того чтобы иметь право распространять и использовать СКЗИ в своей продукции, у компании-производителя прикладного ПО, должны быть необходимые лицензии ФСБ, которые следует регулярно подтверждать.

Виктор Иванов (R-Style Softlab) считает, что российской спецификой рынка ПО для обеспечения информационной безопасности является чрезмерное влияние регулирующих госорганов, которые играют контрольно-распорядительную роль.

Но российская специфика развития рынка имеет и свои достоинства. «Мы на рынок финансовых приложений выходим более защищенными, чем западные банковские системы, которые изначально развивались с ритейла. Вследствие того, что развитие розничных банковских услуг опережало развитие средств обеспечения информационной защиты, ритейловые системы на Западе слабее защищены. Именно поэтому там больше проблем с обеспечением безопасности специализированных приложений», — считает эксперт. Впрочем, эти недостатки могут быть элиминированы путем глубокой интеграции СКЗИ в прикладное ПО.

Существует еще одна принципиальная проблема, связанная с несовершенством законодательной базы. Необходимо определиться, как рассматривать продукты, содержащие встроенные криптоалгоритмы, которые свободно используются на рынке (продукты Microsoft). Получается, что компании, которые продают офисный софт, фактически действуют нелегально, поскольку с этим софтом распространяют и средства криптозащиты (они не являются сертифицированными). Банку, чтобы работать с этими средствами криптографии, нужно получить целый пакет лицензий. В свою очередь, для получения пакета лицензий он обязан использовать только сертифицированные средства. Круг замкнулся. «Фактически, если банк в работе использует Windows, то использует и встроенные в нее криптографические средства. Имеет смысл решить проблему с de jure незаконным использованием «публичной» криптографии и официально дать встроенным средствам «зеленую улицу», — убежден Виктор Иванов (R-Style Softlab).

Есть еще один казус, связанный с использованием криптографических средств. В настоящее время все СКЗИ сертифицируются на три года. Проходит три года, и возникает вопрос, что с таким СКЗИ делать? Распространять это средство криптозащиты нельзя, а вот можно ли использовать? Закон не дает однозначного ответа, что позволяет говорить о еще одной правовой лакуне.

* 1. Рост спроса на биометрию — десятки процентов в год

Инструменты «умной» защиты банков отнюдь не исчерпываются СКЗИ. Наиболее актуальным и во многом еще неосвоенным направлением защиты банковского бизнеса являются, пожалуй, системы биометрической идентификации. Во многом рост популярности биометрии в банковском секторе подстегнуло подчеркнутое внимание к ней со стороны государственных органов стран-лидеров мировой экономики, ставшее следствием глобальной террористической экспансии. Грядущее в России введение биометрических паспортов стимулировало интерес российского бизнес-сообщества в целом и его банковской составляющей в частности к биометрическим системам защиты.

Как рассказал «БО» директор по развитию бизнеса компании BioLink Technologies Дмитрий Кравцов, в последнее время характер интереса банкиров к биометрии разительно изменился. Вопросы уже сводятся не к прикидочному «а что это такое — биометрическая идентификация?», но вполне предметному «что может ваше решение, каковы его характеристики, где и что мы приобретем?». И сегодня представители банковских структур, которые уже попробовали что-то относительно простое, предлагают разработать оригинальную систему на биометрических компонентах, учитывающую тонкости бизнеса именно этого банка.

Какая-либо национальная специфика развития рынка, по мнению Дмитрия Кравцова, отсутствует — вполне типичный бурнорастущий (десятки процентов ежегодно) рынок. За исключением одного принципиального обстоятельства. Холодный климат большинства регионов России повышает требования к аппаратному обеспечению, которое будет установлено на открытом пространстве. Биометрические системы для офиса банка в Сургуте или Ханты-Мансийске должны будут отличаться от их аналогов в Лос-Анджелесе.

«Цены на аппаратное обеспечение в России находятся примерно на том же уровне, что и в остальном мире. Цены же на программную часть системы могут отличаться в разы, причем в России стоимость сложных проектов на сегодня существенно ниже, чем за рубежом», — говорит эксперт.

Что касается потребностей рыночных игроков, то прежде всего банковские структуры интересует защита доступа к важной информации (вход в компьютер, базу данных) по отпечатку пальца или другим биометрическим признакам сотрудников банка. Кроме того, подтверждение транзакций, например, перечисление средств выше определенной суммы, контроль доступа в помещения.

Менее устоявшийся, но быстро растущий спрос отмечается на ряд продуктов, например подтверждение запроса при удаленной работе (выездное отделение банка для выдачи потребкредитов в магазине, салоне). Пользуется спросом учет деловой активности — постоянный контроль за присутствием сотрудника на рабочем месте. При этом коллега-сосед не сможет за сотрудника ввести его пароль или приложить проксимити-карту для отметки присутствия отсутствующего человека. Банки заинтересованы в подтверждении удаленных транзакций для клиентов банка через системы «Банк-Клиент» и идентификации представителей клиентов, приезжающих в банк лично.

Можно утверждать, что риски, например, internet-banking с применением биометрических средств идентификации будут, несомненно, снижены. «Так и хочется сказать, что до нуля, — восклицает Дмитрий Кравцов (BioLink Technologies). — Но! Существуют еще другие проблемы с безопасностью внутри банковских интернет-сервисов, которые зачастую сводят все остальные меры безопасности на нет». Так что, от комплексного решения проблемы безопасности транзакций никак не уйти.

Для того, чтобы биометрия стала неотъемлемой частью такого рода решений, необходим ряд правовых новелл. Должны быть приняты законодательные акты о закреплении биометрических признаков человека в качестве равноправных наряду с бумажными документами для идентификации человека.

Также необходима разработка, утверждение регламентов и системы контроля за их соблюдением. Сегодня не существуeт ни стандартов, по которым должны разрабатываться новые биометрические продукты, ни сертификационных процедур для подтверждения качества таких продуктов.

Было бы несправедливым говорить о том, что в этом направлении ничего не делается. «Наша компания принимает самое активное участие в работе подкомитета по биометрии в рамках технического комитета Росстандарта, который разрабатывает биометрические стандарты для России», — говорит Д. Кравцов. Конечно, достойно сожаления, что согласование требований со стороны различных заинтересованных ведомств продвигается подчас с большим трудом из-за полярности требований.[[2]](#footnote-2)1

* 1. Обеспечиваемая шифром степень защиты

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть (хотя доказать сей факт обычно нельзя). При этом не требуется очень больших усилий для реализации. Единственное, что требуется - это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскрытия системы. Все механизмы, которые могут использоваться для взлома системы надо задокументировать и довести до сведения конечных пользователей.

Теоретически, любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается методом грубой силы (brute force), требуемая мощность компьютера растет экспоненциально с увеличением длины ключа. Ключ длиной в 32 бита требует 2^32 (около 10^9) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битным ключом (например, экспортный американский вариант алгоритма RC4) требуют 2^40 шагов - такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битными ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит вероятно останутся недоступными для вскрытия методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия (считая, что на один шаг затрачивается минимальный квантовомеханический квант энергии) превзойдет массу солнца или вселенной.

Однако, длина ключа это еще не все. Многие шифры можно вскрыть и не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется.

Вообще говоря, следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности, или же надежность зависит от секретности самого алгоритма. Вообще говоря, ни один алгоритм, секретность которого зависит от секретности самого алгоритма не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который дизассемблирует ее и восстановит алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались до смешного ненадежными.

Длины ключей, используемых в криптографии с открытым ключом обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением пары неизвестных простых чисел. В случае некоторых других криптосистем, проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы.

Чтобы дать представление о степени сложности вскрытия RSA, модули длиной 256 бит легко факторизуются обычными программистами. Ключи в 384 бита могут быть вскрыты исследовательской группой университета или компании. 512-битные ключи находятся в пределах досягаемости крупных государств. Ключи длиной в 768 бит вероятно не будут надежны продолжительное время. Ключи длиной в 1024 бит могут считаться безопасными до тех пор, пока не будет существенного прогресса в алгоритме факторизации; ключи длиной в 2048 большинство считает надежными на десятилетия.

Важно подчеркнуть, что степень надежности криптографической системы определяется ее слабейшим звеном. Нельзя упускать из вида ни одного аспекта разработки системы - от выбора алгоритма до политики использования и распространения ключей.[[3]](#footnote-3)1

* 1. Основные цели информационной безопасности

Основными целями информационной безопасности являются:

* сохранение целостности информации в процессе ее хранения, обработки и передачи, обеспечение доступа к ней пользователей в пределах их полномочий;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы;
* сохранение государственной тайны, конфиденциальности информации в документированном и электронном виде в соответствии с законодательством;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* предотвращение незаконного использования информационных ресурсов.

Задачу обеспечения информационной безопасности на конкретной сети передачи данных каждый оператор сети должен решать сам, используя рекомендательные меры и средства защиты информации, руководствуясь при этом действующими нормативными актами.

Для решения задач обеспечения информационной безопасности в области передачи данных и Интернет предусматривается выполнение следующих мероприятий:

* создание узла защиты для сетей передачи данных;
* создание Системы обеспечения информационной безопасности в сфере информационных и компьютерных технологий и формирование служб обеспечения информационной безопасности;
* создание постоянно действующей (межведомственной) экспертной группы для оценки эффективности внедренных средств защиты в сетях передачи данных, проведения экспертизы проектов на соответствие требованиям обеспечения информационной безопасности и разработка рекомендаций по защите информации;
* разработка отечественных средств криптографической защиты информации;
* внедрение систем и средств защиты информации на сетях передачи данных и доступа к сети Интернет;
* обеспечение устойчивости и безопасности функционирования сетей;
* создание центра доверия и выдачи сертификатов, обеспечивающего хранение, генерацию, распределение и определение стойкости ключей, а также выдачу и заверение сертификатов и электронно-цифровой подписи;
* организация структуры по взаимодействию с зарубежными органами по вопросам обеспечения информационной безопасности в сфере компьютерных и информационных технологий;
* создание системы сертификации средств по обеспечению информационной безопасности;
* внедрение системы подготовки и повышения квалификации специалистов по защите информации;
* создание нормативно-правовой базы по информационной безопасности.[[4]](#footnote-4)1

1. Заключение

Криптография - это искусство скрытия информации в последовательности битов от любого несанкционированного доступа. Для достижения этой цели используют шифрование: сообщение с помощью некоторого алгоритма комбинируется с дополнительной секретной информацией (ключом), в результате чего получается криптограмма. Долгое время способы разработки алгоритмов шифрования определялись исключительно хитростью и изобретательностью их авторов. И лишь в ХХ веке этой областью заинтересовались математики, а впоследствии - и физики.

Существует два направления криптографии: банковские криптографические протоколы и криптографическое обеспечение банковских карточек.

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом.

Продукты, защищающие от перехвата конфиденциальных данных, являются одними из самых востребованных сегодня.

Список литературы:

1. Анохин М.И., Варновский Н.П., Сидельников В.М., ЯщенкоВ.В., КРИПТОГРАФИЯ В БАНКОВСКОМ ДЕЛЕ, 2005. – 526 с.
2. algolist.manual.ru/defence/intro.php#strength\
3. tashxis.narod.ru/ru/library/pr1\_200.htm
4. virusunet.ru/sovremennye-sredstva-zashhity.html

1. 1 Анохин М.И., Варновский Н.П., Сидельников В.М., ЯщенкоВ.В., КРИПТОГРАФИЯ В БАНКОВСКОМ ДЕЛЕ, 2005. – стр. 324-325 [↑](#footnote-ref-1)
2. 1 virusunet.ru/sovremennye-sredstva-zashhity.html [↑](#footnote-ref-2)
3. 1 algolist.manual.ru/defence/intro.php#strength [↑](#footnote-ref-3)
4. 1 tashxis.narod.ru/ru/library/pr1\_200.htm [↑](#footnote-ref-4)