**Проблемы информационной безопасности банков**

Диплом

План

Введение

1. 1 глава. Информационные банковские системы – структура и её программно-техническая реализация.
   1. История возникновения банковской системы и её информационной безопасности.
   2. Современное развитие банковской структуры и формирование информационных потоков.
   3. Возможности предоставляемы корпоративными информационными сетями.
      1. Типовая структура корпоративной информационной сети
      2. Применяемая защита корпоративной информационной сети
   4. Анализ потенциальных угроз и проблем информационной безопасности информационным системам
2. 2 глава информационная система банка и её узкие места
3. Заключение
4. Литература

[**Написание на заказ курсовых, дипломов, диссертаций...**](http://учебники.информ2000.рф/napisat-diplom.shtml)

**Вернуться в каталог готовых дипломов и магистерских диссертаций –**

[**http://учебники.информ2000.рф/diplom.shtml**](http://учебники.информ2000.рф/diplom.shtml)

Оглавление

[Введение 3](#_Toc484112183)

[Глава 1. Информационные банковские системы – структура и её программно-техническая реализация. 6](#_Toc484112184)

[1.1. История возникновения банковской системы и её информационной системы. 6](#_Toc484112185)

[1.1. Современное развитие банковской структуры и формирование информационных потоков 8](#_Toc484112186)

[1.2. Возможности предоставляемые корпоративными информационными сетями. 10](#_Toc484112187)

[1.2.1. Типовая структура корпоративной сети 13](#_Toc484112188)

[1.2.2. Защита корпоративных информационных сетей 15](#_Toc484112189)

[1.3. Анализ угроз и проблем информационной безопасности информационным системам 16](#_Toc484112190)

[1.3.1. Потенциальные угрозы информационной безопасности 16](#_Toc484112191)

[1.3.2. Потенциальные проблемы информационной безопасности 19](#_Toc484112192)

[1.4. Типы и используемых локальных сетей 22](#_Toc484112193)

[Глава 2. Анализ информационной банковской системы 26](#_Toc484112194)

[2.1. Описание используемой информационной системы 26](#_Toc484112195)

[2.2. Описание информационной защиты 28](#_Toc484112196)

[Заключение 31](#_Toc484112197)

[Список используемой литературы: 32](#_Toc484112198)

## Введение

Безопасность банковской системы в целом, и каждого отдельного банка, является самой засекреченной информацией в мире, конечно после военной тайны. Финансовые секреты – лакомая добыча заинтересованных организованных групп. От иностранных государств и до преступных элементов, имеются желающие получить незаконным способ текущую информацию. Если в частном банковском секторе утечка секретной информации может привести к банкротству или потерям клиентов, то в государственном масштабе может привести к полному коллапсу всей финансовой системы, что является одной из главных целей подрывной войны против нашего государства.

Из истории развития мировой банковской системы, имеется несколько фактов того, что когда секретная информация становилась достоянием конкурентов, то происходило крушение банковской системы. Одним из примеров имеется крушение крупнейшего банка Венецианской республики, после ого, как через шпионов была добыта информация о крупнейших вложениях. Это было крупнейшей финансовой победой знаменитых Медичи. Точно также в позднейшей истории были факты крахов банков Ост-индийской компании, и в других известных странах Европы, таких как французский банк Ротшильдов.

В современной истории хищение банковской информации принимает другую сторону, в век главенствования всемирной сети Internet, с помощью очень профессиональных людей в информационных технологиях, владеющих способами использования ошибок программного обеспечения, становится очень лёгкой задачей. С помощью хищения информации с банковских карт, происходят списания немаленьких денежных сумм с лицевых счетов клиентов банка.

Также имеется не мало фактов, когда злоумышленники используя социальную психологию получают конфиденциальную информацию от сотрудников определённого банка, и с помощью полученных прав используют информацию в своих целях. Также хакеры похищая, с помощью технических средств, аккаунты пользователей банковских услуг распространяемых при помощи пластиковых карт, снимали с текущих счетов большие денежные суммы.

Приведённые примеры показывают, что при любом техническом прогрессе, используя новейшее программное обеспечение, которое при его эксплуатации допускает появление ошибок при обработке операций, можно получить определённые успехи в проникновении в информационные сети банковского управления. Можно сформулировать мечту современного хакера – с помощью пластиковой карты высокого статуса получить допуск к информационной банковской системе, и прикрываясь легальным допуском использовать права для управления финансовыми потоками.

Настоящий дипломный проект посвящён изучению используемых систем информационной безопасности банковских операций при использовании Сберегательного Банка Северный филиал, г.Ярославль.

В 1 главе настоящего дипломного проекта рассмотрены история создания информационных систем банковской структуры, её прогресс, пример построения корпоративной информационной сети, а также рассмотрены потенциальные угрозы и проблемы возникающие при эксплуатации информационных систем.

Во 2-ой главе рассматривается «идеальная» структура построения информационной банковской системы, её примерная работа (так как если рассматривать фактическую систему работы, то это является разглашением конфиденциальной информации), и предложения об улучшении её работы с небольшим теоретическим проектом.

В заключении подробно рассмотрены полученные выводы об информационных системах банковских структур, её работе, потенциальных угрозах. Актуальность этой работы связана с тем, что в быстроизменяющемся мире происходят различные процессы могущие различными способами модифицировать имеющиеся структуры. Также она показывает, как воспитан технический специалист с профессиональной точки зрения.

## Глава 1. Информационные банковские системы – структура и её программно-техническая реализация.

## История возникновения банковской системы и её информационной системы.

Структура развития коммерческих банков и государственной финансовой системы, объединённой в государственную банковскую систему, идёт по возрастающей восходящей. Опираясь на исторические истоки, видно что превращение меновой системы в компонент превращения материальной формы к её эквиваленту в серебряной мере, а позже золотой, стало прообразом финансовой системы. Она образовалась в течении древнейшей истории, основным фундаментом которой было сбор налогов с населения, когда натуральный продукт был приравнен к официально принятому денежному эквиваленту. Налоговые сборы шли в казну государства, из которой собранные денежные средства тратились, в основном, на государственные нужды, и частично на удовлетворение нужд правящего класса. Эта устоявшаяся система существовала в течении всей древнейшей истории, в разных известных государствах – Древний Вавилон, Древний Египет, Древняя Греция, Персидское царство, Индийские княжества, Китайская Империя, Государства Ацтеков и Инков. Но при историческом прогрессе первые банковские системы стали появляться в средневековой Европе, при начале крестовых походов. Просвещённая Византийская империя, имея колоссальные доходы, не смогла преодолеть ступень в следующем финансовом развитии, которое заключалось в объединении гильдий менял в гильдию хранения, накопления и приумножения денежных средств. Такими центрами финансовых систем стали Венецианская и Генуэзские республики. Именно в них возникли первые банки, в которых крестоносцы хранили свои денежные средства, а также полученную добычу. Используя полученный опыт, коммерческие банки стали возникать и в других средневековых странах. Тогда же стали появляться шпионские центры по добыче ценной информации о крупнейших вкладчиках, с целью последующего изъятия денежных средств в свою пользу. Таким образом, в течении всего исторического развития Европейских государств, параллельно с ними развивались и коммерческие банки. История возникновения государственных банков началась с середины 17 века. Именно в это время, при достижении полнейшей централизации государств, при фискальной системе, стали возникать государственные банки. Их основным определением было управление финансами государства с целью его дальнейшего развития при промышленном развитии. Собираемые налоги скапливались в казне государства, потомком которой стали государственные банки, которые под управлением особо доверенных людей царствующих особо того времени вкладывались в развитие экономики государств. Именно эти государственные образования, стали главной целью финансовой разведки государств – противников.

Сама система работы коммерческого банка со вкладчиками стала формироваться именно в это время. В структуре появилось правление, так как один человек, не мог создать банк, в него входило несколько человек – учредителей. Так как денежные средства получали от населения, то сформировалась структура работы со вкладчиками. Эта структура принимала денежные средства на определённый срок – взамен вручая заверенные расписки, и выдавала на определённый срок – так же вручая заверенные расписки. Так как банк не мог работать без прибыли, то на такие операции начислялись проценты, или ростовщичество. Кроме того, в структуре появилась система филиалов, отделения банка открывались во всех крупных городах страны, и они могли принимать для оплаты расписки выданные разных городах. Также создался отдел валютных операций, обмен одной валюты на другую. И коммерческий отдел – сами денежные средства вкладывались в развитие либо предприятий, либо торговли, либо снаряжались морские караваны для открытия новых земель.

Рисунок 1 Структура коммерческого банка в период новой истории

Работа со вкладами

Валютно-обменные операции

Коммерческие операции

Промышленно-финансовая разведка и шпионаж

Контрразведка и охрана

## Современное развитие банковской структуры и формирование информационных потоков

При дальнейшем историческом развитии, в связи с промышленной революцией и освоением Нового Света, а так же развитием торговли, параллельно развивалась и банковская система. С развитием колониальной системы, коммерческие банки открывали свои филиалы и представительства в новых городах и странах. Это способствовало тому, что развивалась система получения отчётов и приказов между метрополией и дочерней структурой. Для этого в структуре создавались новые отделы с функциями издания, получения и хранения отчетно-финансовой документации. Так же стало развиваться акционерное направление связанное с выпуском и размещением на вновь образованной бирже акций предприятий. Так как акции представляли собой гарантийную бумагу с передачей части стоимость предприятия новому владельцу, то были созданы отделы по работе с биржами и размещением акций.

Обособленно было выделено бухгалтерское обеспечение деятельности банка. И соответственно возрос поток обмена информацией между структурными подразделениями и созданием полного отчёта для предоставления в правление банка.

Работа со вкладами

Валютно-обменные операции

Коммерческие операции

Промышленно-финансовая разведка и шпионаж

Контрразведка и охрана

Биржа

Акции и ценные бумаги

Бухгалтерия

Филиалы и представительства

Рисунок 2 Структура коммерческого банка на начало ХХ века

Эта структура сохранилась практически без изменения до середины ХХ века, пока не стали применяться Электронно-Вычислительные машины. Это создало новые возможности в обработке коммерческой информации. С развитием электронных технологий нашло своё применение и революционная система внутренних сетей для централизованного получения и хранения информации. Дальнейшее развитие системы обработки информации, появление персональных ЭВМ и объединение рабочих мест в отделах в локальные сети, и дальнейшее объединение отдельных локальных сетей обмена информации в общую сеть предприятия создало полноценную современную структуру банковских информационных потоков.

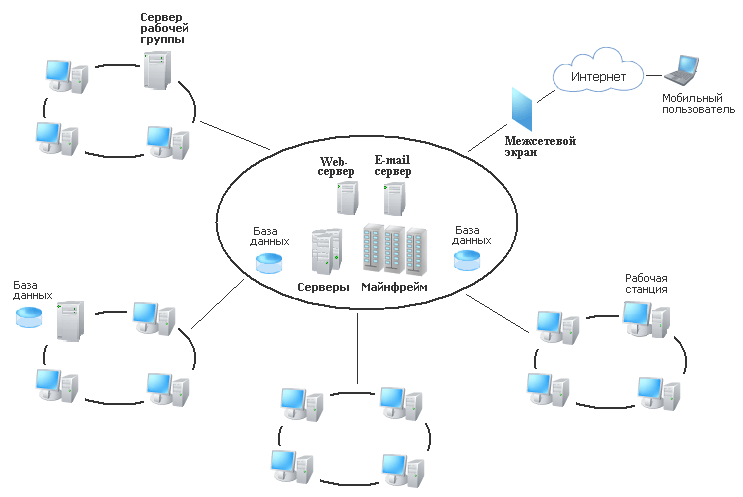


Рисунок 3 современная структура банковской системы обмена информации

Потоки информационной системы финансово-кредитного учреждения, на данный момент, характеризуются направлением, структурой, периодичностью, видом носителя данных, способом индикации, степенью взаимосвязи потока, объёмом, плотностью отдельных сообщений, методом образования, способом и степенью использования данных потока[[1]](#footnote-1).

## Возможности предоставляемые корпоративными информационными сетями.

Корпоративная сеть может предложить следующие возможности:

* Единое информационное пространство;
* Оперативность получения информации и возможность формирования консолидированных отчётов уровня предприятия или объединения предприятий;
* Централизация финансовых и информационных потоков данных;
* Возможность оперативного сбора и обработки информации;
* Снижение затрат при использовании серверных решений. Переход решений от рабочих групп на решения на уровне предприятия;
* Возможность обработки мультимедийных потоков данных между офисными площадками;
* Снижение затрат на связь между подразделениями фирмы, организация единого номерного пространства;
* Возможность организации системы видеонаблюдения на основе IP сети предприятия.

Название корпоративная сеть появилось в силу того, что под понятием корпорация стали подразумевать объединение большого количества пользовательских станций используемых в одном конгломерате профессиональной деятельности.

При создании корпоративных сетей используются различные технологии или их комбинации: от кабельных и беспроводных систем до инновационных технологических решений. К ним относятся специальные решения на уровне серверных станций, специального программного обеспечения, развития технологий защиты данных от хищения и вирусной опасности, а также противодействие промышленному шпионажу. Чаще всего для достижения оптимального решения используют комбинацию нескольких технических решений, у каждого из которых есть свои преимущества и недостатки.

В настоящее время в корпоративные сети могут входить не только отдельные рабочие группы, локальные вычислительные сети, но и удалённые подразделения, объединённые общей сетью Internet или выделенными каналами. Удалённый доступ к используемым ресурсам предприятия могут получить, предварительно получив разрешение и право доступа, как партнёры организации, так и сотрудники вне офиса. Одним из факторов широкого применения корпоративных сетей, стало распространение удалённых сотрудников, которые исполняют свои обязанности территориально не находясь на своём рабочем месте. Эта инновация даёт возможность предприятиям сокращать работников на местах, переводя их на должности удалённых работников.

При этом используется эффективная обеспеченная информационная безопасность и защита сервисов и услуг, предоставляемых авторизованным пользователям, от несанкционированного доступа и атак, направленных на выведение сервисов из строя.

На основании научно-обоснованных решений и разработок, можно сказать, что корпоративные сети являются технически сложными системами, включающими в себя тысячи разнообразных элементов и компонентов: ПЭВМ разных типов, начиная с настольных и заканчивая мэйнфреймами, системное и прикладное программное обеспечение, сетевая инфраструктура, такая как – сетевые адаптеры, концентраторы, маршрутизаторы, файерволы и системы защиты. Особую роль играет специализированное программное обеспечение. Интенсификация применения приложений на основе WEB-сервисов одновременно упрощает и усложняет развитие инфраструктуры. Интенсивное обращение к внешним WEB-сайтам увеличивает долю внешнего трафика, и соответственно повышает нагрузку на пограничные маршрутизаторы и межсетевые экраны корпоративной сети. С другой стороны применение сайтовой структуры внутри корпорации, при которой расширены службы INTRANET и предлагается доступ к внутрикорпоративным сайтам с возможностью передачи и получения информации адресно и практически мгновенно, с использованием внутреннего аккаунта и веб-страницы с заданиями и отчетами выполненными и находящимися в работе, актуализирует индивидуальный и групповой подход к решениям сиюминутных задач.

Также большое влияние на бизнес процессы оказано в структуре аутентификации и авторизации большого числа клиентов обращающихся на серверы предприятий из вне и внутри. Здесь имеется применение новых методов проверки легальности пользователей.

Из этих особенностей появились основные характеристики корпоративных сетей. Это требования предъявляемые к ним, главное из них: обеспечение пользователям возможности оперативного доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть.

Из этого требования, вытекают и другие – по производительности, надежности системы, безопасности доступа и обработки, управляемости и конфигурируемости, совместимости с различными версиями, расширяемости, масштабируемости и прозрачности. Качество предоставления услуг корпоративной сетью определяется тем, насколько полно выполняются эти требования, особенно по производительности и надежности.

Из удовлетворения этих требований и формируется оценка эксплуатации корпоративной информационной сети.

### Типовая структура корпоративной сети

Для корпоративных сетей крупных предприятий или высшего ранга являются характерными черты:

* Масштабность – включают в себя сотни и тысячи рабочих станций, наличие удаленных станций для работы сотрудников, десятки и сотни серверов, большие объемы компьютерных и мультимедийных данных, множество разнообразных приложений;
* Гетерогенность – возможность использования различных типов компьютеров и рабочих станций, коммуникационного оборудования, операционных систем и приложений;
* Использование территориальных сетей связи – удаленные филиалы и отделения соединяются между собой и центральным офисом с помощью телекоммуникационных средств, в том числе телефонных каналов, радиоканалов, спутниковой связи;
* обеспечение поддержки различных видов трафика, организация виртуальных локальных сетей для оперативного взаимодействия сотрудников предприятия в рамках рабочих групп «по интересам», управляемость, расширяемость, масштабируемость, безопасность информации в сети.

Корпоративная сеть для крупномасштабной корпорации обычно состоит из нескольких локальных сетей (подсети) и серверов, управляющих связей между ЛКС. Каждая ЛКС обслуживает отдельного подразделения или филиала корпорации.

Для организации связи между удаленными подразделениями строится магистральная сеть. Может быть выполнена в виде выделенной линии, оптико-волоконной линией или с использованием виртуальной сети.

Для выхода на магистральную сеть используется сеть Internet. Серверы обращений управляют связями между центральным сервером и локальными серверами. Корпоративные серверы выполняют такие функции как: работа с центральной базой данных (сервер БД), управление электронным документооборотом, управление электронной почтой, управление выходом в Internet и т.д.

### Защита корпоративных информационных сетей

К защите корпоративных сетей, от несанкционированного доступа, хакерских атак, изменения данных и других опасных методов предлагаются две достаточно больших и независимых групп технических решений примененных к информационным технологиям.

* Технология обеспечения гарантированного уровня транспортного обслуживания (качества сервиса) для корпоративного трафика, транспортируемого через публичные сети;
* Технология обеспечивающая необходимые гарантии информационной безопасности(конфиденциальности и целостности) корпоративных данных, передаваемых через публичные сети.

Так как приняты корпоративные сети на основе VPN, то к первой группе имеют отношения специализированные технологии управления качеством обслуживания RSVP, DiffServ, MPLS, и базовые технологии построения публичных сетей скорректированные встроенными элементами поддержки QoS.

Для второй группы VPN-технологии, имеется отличие в том, что выполняется функция авторизации абонентов корпоративных сетей и функций криптографической защиты передаваемых данных. К этой группе относятся различные реализации механизма инкапсуляции стандартных сетевых пакетов канального (PPTP, L2F, L2TP) сетевого (SKIP,IPSec/IKE) и уровней модели OSI/ISO(SOCKS, SSL/TLS).

Исходя из этого предусматривается построение VPN на базе сетевой ОС, что является достаточно удобным и дешевым средством создания защищенной инфраструктуры виртуальных каналов. Или построение VPN на базе маршрутизаторов, наиболее практичным является использование решений на базе CISCO.

Вне зависимости от выбора системы построения, защита данных является приоритетной задачей службы безопасности корпоративной сети. Дополнительно использующей разные антивирусные меры защиты основанной на разработках производителей ПО антивирусов.

## Анализ угроз и проблем информационной безопасности информационным системам

### Потенциальные угрозы информационной безопасности

К потенциальным угрозам могущим нанести огромные финансовые и имиджевые убытки, по классификации служб информационной безопасности, могут относится следующие классы:

Получение доступа к сетевым сервисам используемым при работе банка и его офисов через открытые сети:

* Несанкционированный доступ к ресурсам и данным системы (подбор пароля, взлом систем защиты и администрирования, действия от имени чужого лица (маскарад));
* Перехват и подмена трафика (подделка платежных поручений, атака типа «человек посредине»);
* IP-спуфинг (подмена сетевых адресов);
* отказ в обслуживании;
* атака на уровне приложений;
* сканирование сетей или сетевая разведка;
* использование отношений доверия в сети.

Целенаправленные атаки на финансовые сообщения и финансовые транзакции:

* раскрытие содержимого;
* представление документа от имени другого участника;
* несанкционированная модификация;
* повтор переданной информации.

Хакерские атаки:

* рассылка спама и внедрение вредоносных программ посредством электронных писем с предложениями сотрудничества;
* перехват и перенаправление сетевого трафика на поддельные сетевые ресурсы с целью завладения ценной информацией;
* DDOS-атаки с целью переполнения стека информации и автоматического его закрытия управляющим сервером, что приводит к полной потере трафика.

Данные угрозы могут возникнуть в силу разных причин, а также могут являться следствием плохой организации производственного процесса.

К ним относятся - слабая готовность персонала, обслуживающего технические средства обработки информации, отсутствие необходимых средств контроля и информационной защиты, отсутствие или неполная проработка концепции информационной безопасности организации, а также неадекватная реализация предписаний политики: неумение реализовать систему разделения доступа, обновления паролей и ключевых слов, а также неспособность или неподготовленность осуществить администрирование и настройку использующихся сетевых сервисов.

Службы безопасности также классифицируют потенциальных нарушителей безопасности, которые делятся на:

- внешних и внутренних нарушителей:

* к внутренним относятся сотрудники самого банка или сотрудники организаций из сферы ИТ, предоставляющие банку телекоммуникационные или иные информационные услуги.
* К внешним нарушителям могут относится:

- клиенты (имеющие разные цели нанесения вреда);

- приглашенные посетители;

- представители конкурирующих организаций;

- сотрудники органов ведомственного надзора и управления;

- нарушители пропускного режима;

- наблюдатели за пределами охраняемой территории.

Способы и методы используемые для причинения вреда:

* сбор информации и данных;
* пассивные средства перехвата;
* использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;
* активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных.

Имеющийся уровень знаний об организации информационной структуры, для максимального нанесения вреда:

* типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;
* высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;
* высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;
* обладание сведениями о средствах и механизмах защиты атакуемой системы;
* нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.
* Время информационного воздействия:
* в момент обработки информации;
* в момент передачи данных;
* в процессе хранения данных (учитывая рабочее и нерабочее состояния системы).

Подход к выбору осуществления вредоносного воздействия:

* удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;
* доступ на охраняемую территорию;
* непосредственный физический контакт с вычислительной техникой, при этом можно выделить:
* доступ к терминальным операторским станциям,
* доступ к важным сервисам предприятия (сервера),
* доступ к системам администрирования, контроля и управления информационной системой,
* доступ к программам управления системы обеспечения информационной безопасности.

### Потенциальные проблемы информационной безопасности

При создании любой информационной системы (ИС) на базе современных компьютерных технологий неизбежно возникает вопрос о защищённости этой системы от внутренних и внешних угроз безопасности информации.

Но прежде чем решить, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информации на предприятии и оценить степень защищённости информационных активов.

Для этого проводится комплексное обследование защищённости ИС  
(или аудит безопасности), основанные на выявленных угрозах безопасности информации и имеющихся методах их парирования, результаты которого позволяют:

* оценить необходимость и достаточность принятых мер обеспечения
* безопасности информации;
* сформировать политику безопасности;
* правильно выбрать степень защищённости информационной системы;
* выработать требования к средствам и методам защиты;
* добиться максимальной отдачи от инвестиций в создании и обслуживании СОБИ.

Данные мероприятия помогают выявить потенциальные проблемы информационной безопасности, такие как:

1. Доступ к сервисам, которые предоставляет данное программное обеспечение, осуществляется через открытые сети, использование которых таит в себе многочисленные информационные угрозы.

Выявить причины, которые могут привести к появлению уязвимостей:

* отсутствие гарантии конфиденциальности и целостности передаваемых данных;
* недостаточный уровень проверки участников соединения;
* недостаточная реализация или некорректная разработка политики безопасности;
* отсутствие или недостаточный уровень защиты от несанкционированного доступа (антивирусы, контроль доступа, системы обнаружения атак);
* существующие уязвимости используемых операционных систем (ОС), ПО, СУБД, веб-систем и сетевых протоколов;
* непрофессиональное и слабое администрирование систем;
* проблемы при построении межсетевых фильтров;
* сбои в работе компонентов системы или их низкая производительность;
* уязвимости при управлении ключами.

1. Для поиска слабых мест для атак на финансовые сообщения и финансовые транзакции, проверяется наличие применения следующих средств:

* шифрование содержимого документа;
* контроль авторства документа;
* контроль целостности документа;
* нумерация документов;
* ведение сессий на уровне защиты информации;
* динамическая аутентификация;
* обеспечение сохранности секретных ключей;
* надежная процедура проверки клиента при регистрации в прикладной системе;
* использование электронного сертификата клиента;
* создание защищенного соединения клиента с сервером.

На основании выполненных проверок по имеющейся информационной безопасности стандартными способами являются применение следующих видов защиты информации:

Комплекс технических средств защиты интернет-сервисов:

* брандмауэр (межсетевой экран) — программная и/или аппаратная реализация;
* системы обнаружения атак на сетевом уровне;
* антивирусные средства;
* защищенные ОС, обеспечивающие уровень В2 по классификации защиты компьютерных систем и дополнительные средства контроля целостности программ и данных;
* защита на уровне приложений: протоколы безопасности, шифрования, ЭЦП, цифровые сертификаты, системы контроля целостности;
* защита средствами системы управления БД;
* защита передаваемых по сети компонентов программного обеспечения;
* мониторинг безопасности и выявление попыток вторжения, адаптивная защита сетей, активный аудит действий пользователей;
* обманные системы;
* корректное управление политикой безопасности.

При проведении электронного документооборота должны выполняться:

* аутентификация документа при его создании;
* защита документа при его передаче;
* аутентификация документа при обработке, хранении и исполнении;
* защита документа при доступе к нему из внешней среды.

## Типы и используемых локальных сетей

На основании научно-обоснованных решений и разработок, можно сказать, что корпоративные сети являются технически сложными системами, включающими в себя тысячи разнообразных элементов и компонентов: ПЭВМ разных типов, начиная с настольных и заканчивая мэйнфреймами, системное и прикладное программное обеспечение, сетевая инфраструктура, такая как – сетевые адаптеры, концентраторы, маршрутизаторы, файерволы и системы защиты. Особую роль играет специализированное программное обеспечение. Интенсификация применения приложений на основе WEB-сервисов одновременно упрощает и усложняет развитие инфраструктуры. Интенсивное обращение к внешним WEB-сайтам увеличивает долю внешнего трафика, и соответственно повышает нагрузку на пограничные маршрутизаторы и межсетевые экраны корпоративной сети. С другой стороны применение сайтовой структуры внутри корпорации, при которой расширены службы INTRANET и предлагается доступ к внутрикорпоративным сайтам с возможностью передачи и получения информации адресно и практически мгновенно, с использованием внутреннего аккаунта и веб-страницы с заданиями т отчетами выполненными и находящимися в работе, актуализирует индивидуальный и групповой подход к решениям сиюминутных задач.

Также большое влияние на бизнес процессы оказано в структуре аутентификации и авторизации большого числа клиентов обращающихся на серверы предприятий из вне и внутри. Здесь имеется применение новых методов проверки легальности пользователей.

Из этих особенностей появились основные характеристики корпоративных сетей. Это требования предъявляемые к ним, главное из них: обеспечение пользователям возможности оперативного доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть.

Из этого требования, вытекают и другие – по производительности, надежности системы, безопасности доступа и обработки, управляемости и конфигурируемости, совместимости с различными версиями, расширяемости, масштабируемости и прозрачности. Качество предоставления услуг корпоративной сетью определяется тем, насколько полно выполняются эти требования, особенно по производительности и надежности.

Совокупность всего вышеперечисленного формирует работоспособность корпоративной сети, которая обеспечивается тремя основными компонентами:

1) Хранение данных;

2) Поиск и обработка данных;

3) Интерфейс пользователя.

Эти компонент реализуются независимо друг от друга, но четко взаимодействуют между собой. Имеется зависимость от того, в скольких уровнях организованы эти компоненты и как распределяются функции между ними. Исходя из этого выделены два вида архитектуры корпоративных сетей: двухуровневая и многоуровневая.

Двухуровневая архитектура представлена реализацией «файл-сервер» и «клиент-сервер». В этом случае три основных компонента физически распределяются между двумя модулями (уровнями).

Обычно архитектура «файл-сервер» реализуется в локальной компьютерной сети, где один уровень является файл-сервером, местом хранения файлов пользователя, а другой клиентом – самим пользователем.

Архитектура «клиент-сервер» реализуется при помощи специализированной СУБД, и разделяется на две части: серверную и клиентскую. В этом случае, клиент, организованный на 1-ом (нижнем) уровне обращается к службам, которые организованы на 2-ом (верхнем) уровне.

Многоуровневая архитектура корпоративной сети, может быть представлена классической формой являющейся трехуровневой архитектурой. В ней на среднем (промежуточном) уровне организован прикладной сервер, на котором реализованы как логика приложений, так и операции по управлению данными. На нижнем уровне реализованы запросы и интерфейсы пользователей, которые состоят из средств представления, логики представления и программных интерфейсов для обращения к серверу приложений, расположенного на среднем уровне. Верхний уровень состоит из сервера базы данных, выполняющего операции с БД и файлами.

Таким образом в многоуровневой системе, на нижнем уровне обслуживаются запросы клиентов и реализуются интерфейсы пользователей, на втором уровне выполняется обработка данных при помощи прикладных программ, а на верхнем уровне реализованы БД и соответствующая ей СУБД. Каждый уровень реализуется на отдельном компьютере.

Более современной является архитектура, построенная на основе использования Internet\Intranet технологий. Она реализована на объединении многоуровневой архитектуры с технологиями Internet/Intranet. Схема её построения следующая:

* Браузер-сервер являющийся интерфейсом сервера-приложений
* Сервер приложений – сервер баз данных(БД)
* Сервер баз данных – сервер динамических страниц – Web- сервер.

Благодаря этой интеграции Internet-технологии с многоуровневой архитектурой, корпоративные сети более упрощаются в применении и сопровождении. Они работают с информацией удобной для непрофессиональных пользователей. Именно эти системы объединяют в себе самые положительные стороны многопользовательских систем и систем «клиент-сервер». Они обладают следующими особенностями:

- для использования на сервере накапливаются не данные, а информация;

- клиент и сервер, при обмене информацией, используют стандартный протокол;

- потому как прикладная система расположена на сервер, пользователю для работы, на клиентском компьютере, достаточно иметь программный навигатор с отображением динамической страницы.

## Глава 2. Анализ информационной банковской системы

Моделью для исследования является Северный банк Сберегательного Банка РФ. Адрес: 150003, Ярославская обл., г. Ярославль, проспект Октября, д. 8 телефон (4852)407811.

Основанием для исследования данного объекта, явился тот факт, что он является головным банком для нескольких областей Российской Федерации, имеет на своем техническом вооружении современное оборудование, имеет большую информационную систему связи со своими подчиненными филиалами посредством привлечения всех имеющихся, на настоящие время, форм связи. И на его примере можно рассмотреть все проблемы, означенные в данном дипломном проекте.

## Описание используемой информационной системы

Организационная структура исследуемого объекта состоит из следующих отделов:

1. Руководства
2. Отдела бухгалтерского учета и отчетности
3. Отдела расчета и переводов
4. Отдела вкладов
5. Коммунального отдела
6. Отдела кредитования
7. Отдела службы безопасности
8. Отдела кадров
9. Отдела ценных бумаг
10. Отдела валютного контроля
11. Валютного отдела
12. Экономического отдела
13. Юридического отдела.
14. Отдела информационных технологий
15. Инкассаторского отдела

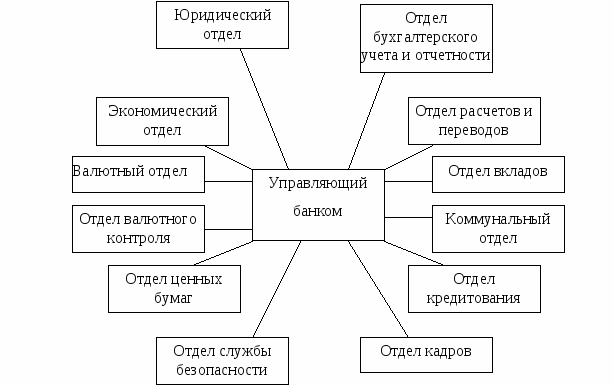


Рисунок 4 Организационная структура филиала банка

Приведённая структура является схематической и не отражает истинного структурного разделения.

На основании организационной структуры также сформирована и внутренняя локальная сеть. Локальная сеть построена на использовании системы «Сервер – клиент». Это проверенная система, которая стабильно работает. Основана на применении оптико-волоконной связи с большой пропускной системой. Серверное ПО Microsoft Server 2012 основано на применении мэйнфреймов с большим дисковым пространством и большим количеством процессоров Xenon.

В систему отдельно выделены локальные сети отделов, которые расписаны в отдельные подсети, с непересекающимися IP-адресами. Часть персональных компьютеров, работающих с конфиденциальными данными выделены в бездисковые рабочие станции. На остальных пользовательских компьютерах развернуты Windows 7 SP2. Для обеспечения безопасности развернуты Active Directory, файервол на базе Cisco.

## Описание информационной защиты

Доступ к информационной банковской система развернут на основании работы Active Directory. Эта система представляет собой идентификацию пользователя по его аккаунту, введенную в базу данных. При работе с аккаунтом прописываются допуски пользователя к информационным ресурсам. На пример работник отдела кадров не попадет в систему бухгалтерского учета, даже если он зайдет в систему со своим паролем. Допуск к использованию документов организован на системе LOTUS, в которой каждый документ закреплен за своим пользователем. Так же ведутся логические записи о входе-выходе пользователя системы и какими документами он пользуется. В отделах среднего звена работающих по своим направлениям, начальники отделов, имеющие право подписи выходных документов используют ключ-таблетку ля пользования своим рабочим местом. Все финансовые документы проходят через логико-параметрический контроль и подписываются цифровой подписью. Алгоритм которой меняется каждые сутки. Реализован механизм подтверждения полученных/оправленных документов посредством связи с отправителем и подтверждение ХЕШ-суммы MD. Внутри офиса действует беспроводная сеть Вай-Фай, позволяющая служащим получать на рабоие планшеты всю информацию необходимую им при работе с клиентами в отдалении от рабочих мест. Доступ к сети так же запаролен, и не имеет гостевого входа.

Для контроля за копированием электронных документов, в рабочих станциях физически отключены порты USB, кроме двух – при обращении к которым посредством специально разработанной Сберегательным банком программы фиксируются копирование/передача данных с носителя.

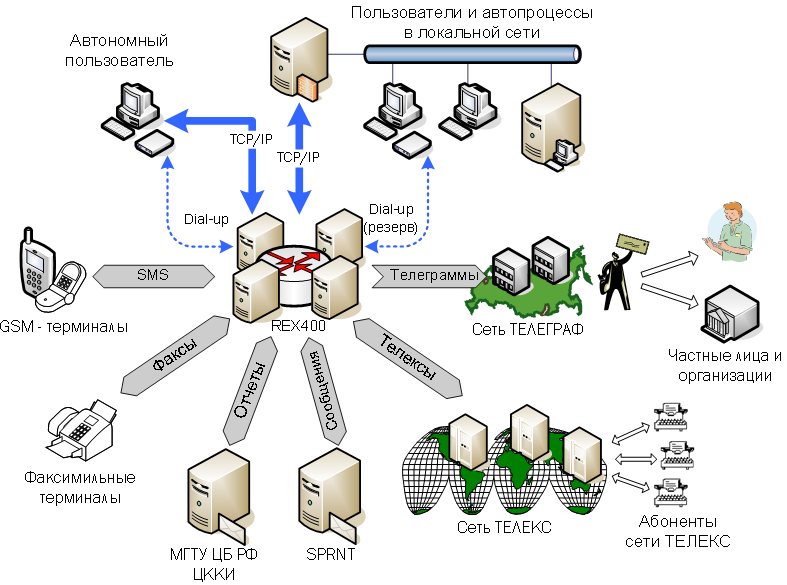


Рисунок 5 схема работы внутренней информационной сети

Работа с филиальной структурой основана на применении выделенных сетей которые защищены посредством применения VPN. Обмен информацией происходит посредством её кодирования через шифроблок (криптосервер), эти блоки синхронизированы между собой и работают синхронно с выделенным ему филиалом.

Для работы с удаленными пользователями и банкоматами выделены радиочастоты с плавающей частотой. Особо это построено для получения информации в реальном времени от терминалов и банкоматов. Так как вся информация о пластиковых картах хранится в центральном информационном хранилище, то происходит передача запроса о использовании пластиковой карты, подтвержденной вводом PIN-кода. Запись транзакций об операциях также происходит через выделенный радиоканал.

Система работы с банкоматом основана на том, что операционная система банкомата принимает и передает считанную информацию не храня её в своей памяти.

Применение антивирусной политики основано Применение антивирусов для межсетевых экранов на сегодняшний день сводится к осуществлению фильтрации доступа в Интернет при одновременной проверке на вирусы проходящего трафика. Также защищают файл-серверы, сервера баз данных и сервера систем коллективной работы, поскольку именно они содержат наиболее важную информацию. антивирусной защите подлежат все компоненты банковской информационной системы, связанные с транспортировкой информации и/или ее хранением:

* Файл-серверы;
* Рабочие станции;
* Рабочие станции мобильных пользователей;
* Сервера резервного копирования;
* Сервера электронной почты;

Отдел информационной защиты прилагает большие усилия по отработке потенциальных угроз нарушения информационной, и проводит следующие мероприятия:

* организацию режима и охраны для исключения возможности тайного проникновения на территорию и в помещения посторонних лиц;
* организацию работы с сотрудниками по обучению правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации;
* организацию работы с документами, включая разработки и использование документов и носителей КИ, их учет, исполнение, возврат, хранение и уничтожение;
* организацию использования технических средств сбора, обработки, накопления и хранения КИ;
* регламентация разрешительной системы разграничения доступа персонала к защищаемой информации;
* организация ведения всех видов аналитической работы;
* регламентация действий персонала в экстремальных ситуациях;
* регламентация организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;
* организация защиты информации – создание службы информационной безопасности или назначение ответственных сотрудников за защиту информации.

## Предложения по усилению защиты информационной системы

В основу построения информационной системы положен принцип создания единого информационного пространства, обеспечивающего информационную поддержку принятия решений в сферах банковской информационной системы.

Оперативное взаимодействие и обмен информацией между субъектами информационной системы осуществляется через Интернет с помощью технического оператора, в функции которого входит:

- сопровождение сервера центральной базы данных;

- предоставление интерфейсов доступа к данным;

- обеспечение достоверности данных и их защита при передаче, обработке и хранении.

Централизация хранения критичных для принятия решений об банковских операциях и передача их через Интернет сопряжены с угрозами сохранности и достоверности данных, что требует принятия комплекса мер по обеспечению их защиты.

По используемым сетевым протоколам методы передачи данных в ИАС МЛГ ВС можно разделить на три группы:

1. Веб-приложения передающие данные по протоколу HTTP (англ. HyperText Transfer Protocol – "протокол передачи гипертекста").

2. Обмен данными через криптотуннель , основанный на протоколе SCP (англ. Secure Copy – "безопасное копирование"), с использованием в качестве транспортного протокола SSH (англ. Secure SHell – "безопасная оболочка").

3. Электронная почта, передаваемая по протоколу SMTP (англ. Simple Mail Transfer Protocol – простой протокол передачи почты).

Электронная почта, являясь наиболее доступным методом для пользователей, не владеющих информационными технологиями, имеет множество недостатков. Их можно частично компенсировать с помощью дополнительного программного обеспечения (ПО) шифрования и электронной цифровой подписи (ЭЦП), но это нецелесообразно, так как делает передачу данных более сложной по сравнению с использованием других методов.

**Шифрование Интернет – трафика**

Веб-приложения защищаются от перехвата и подмены трафика использованием расширения протокола HTTP, известного как HTTPS (англ. HyperText Transfer Protocol Secure – безопасный протокол передачи гипертекста). Трафик шифруется по алгоритму AES (англ. Advanced Encryption Standard – улучшенный стандарт шифрования) с использованием 256-битного ключа. В соответствии с протоколом HTTPS, подключаясь к серверу, браузер должен:

1) убедиться, что на запрос по доменному имени bank.ru отвечает сервер Сберегательного Банка, а не подставной сервер злоумышленников, изменивших запись на ближайшем к пользователю сервере доменных имён (DNS);

2) безопасно передать серверу случайным образом сгенерированный для текущего сеанса ключ симметричного шифрования, которым сервер сможет дешифровать передаваемые данные.

Обе задачи решаются использованием SSL-сертификата, полученного Сберегательным банком от компании Thawte Inc., имеющей статус корневого удостоверяющего центра. Этот сертификат содержит открытый ключ сервера, которым браузер зашифровывает сеансовый ключ. Расшифровать сеансовый ключ (а с его помощью и передаваемые данные) можно только посредством парного закрытого ключа.

Обмен данными через криптотуннель, автоматизирующий передачу больших объёмов данных, обеспечивает шифрование всего трафика по алгоритмам AES с 256-битным ключом, которое является неотъемлемой составляющей используемого транспортного протокола SSH.

**Авторизация пользователей**

Авторизация пользователей представляет собой процесс проверки прав на получение или отправку в сертификационный центр Сербанка определённой категории данных. Список прав доступа каждого пользователя хранится в базе данных.

Веб-приложения авторизуют пользователей по вводимому логину и паролю. Для предотвращения подбора пароля доступ к серверу блокируется несколько минут после пятой неудачной попытки авторизации. Авторизованный в одном приложении пользователь идентифицируется другими приложения без ввода пароля по коду сессии, передаваемому с помощью технологии так называемых "cookie".

Сквозная авторизация не означает получения полного доступа ко всем приложениям. В каждом приложении любое обращение к данным предваряется идентификацией пользователя по коду сессии с проверкой прав доступа к конкретной категории данных, что также защищает от взлома путём подмены содержимого HTTP-запросов.

В процессе авторизации вместе с логином и паролем браузер передаёт серверу номера версий компонентов веб-приложения. Это позволяет с помощью описанного в алгоритма предотвратить потерю данных в случае, когда разработчики меняют формат записей базы данных и обновляют код веб-приложения на сервере. Без принятия соответствующих мер браузер пользователя не сразу загружает обновлённый код, продолжая выполнять старый, сохранившийся в кэше браузера или прокси-сервера, и отправляя данные на сервер в старом несовместимом формате.

Также в процессе авторизации от браузера принимаются и сохраняются данные о версиях пользовательской операционной системы (ОС), прокси-сервера и конфигурации браузера, что упрощает локализацию проблем при оказании пользователям технической поддержки.

Обмен данными через криптотуннель для подтверждения подлинности пользователя использует 1024-битный ключ RSA, который передаётся субъекту сбербанка в составе пакета клиентского ПО, обеспечивая более надёжную авторизацию пользователя по сравнению с использованием пароля. Встроенные в SSH-сервер средства защиты блокируют доступ в случае попыток перебора ключа авторизации. SSH-сервер сконфигурирован только для передачи файлов, функции терминального доступа и переназначения TCP-портов заблокированы.

**Защита от несанкционированного доступа в обход интерфейсов**

Центральная база данных сбербанка, расположенная в локальной вычислительной сети (ЛВС) имеет два рубежа защиты от несанкционированного доступа к данным из Интернета Внутренний рубеж защиты образуется разделением серверов на две группы:

1. Серверы, хранящие полный набор данных (базы данных, файловый архив фотографий пономерной документации компонентов ВС). Эти серверы, обрабатывающие данные и формирующие отчётную документацию, работают на ОС Microsoft Windows, используя такие преимущества платного ПО, как дружественный интерфейс, простота интеграции с корпоративными системами, наличие мастеров и конструкторов для быстрого решения прикладных задач.

2. Серверы Интернет-интерфейсов (веб-приложений и обмена данными через криптотуннель), включая вспомогательные файл-сервер и сервер баз данных, используемые в качестве буфера для временного хранения ограниченного набора данных. Эта группа серверов работает под управлением ОС GNU/Linux, используя такие преимущества свободного ПО с открытым исходным кодом, как меньшая уязвимость к сетевым атакам, высокая стабильность и очень подробное журналирование ошибок и отладочной информации, необходимое для диагностики проблем, возникающих у удалённых пользователей.

Данные между двумя группами серверов передаются исключительно посредством выполняемых по расписанию программ-репликаторов, алгоритмы которых исключают возможность попадания произвольных данных из ЦБД в доступные через Интернет-серверы.

Внешний рубеж защиты создаётся маршрутизатором Cisco Systems, предоставляющим доступ из Интернета только к рабочим портам веб- и SSH-серверов, и инспектирующим весь остальной трафик по технологии CBAC (Context-Based Access Control), блокируя любые входящие сетевые пакеты, не являющиеся ответами на исходящие из ЛВС запросы.

**Построение отказоустойчивой системы хранения и обработки данных**

Классическая серверная архитектура, при которой каждый физический сервер работает под управлением одной ОС с установленным набором приложений, не позволяет быстро восстановить работоспособность приложений в случае отказа сервера. Даже при наличии свободного запасного сервера установка и конфигурирование ОС и приложений потребует нескольких часов. При этом оперативное восстановление данных не всегда возможно, например, в случае выхода из строя снятого с производства контроллера отказоустойчивого дискового массива.

Для предотвращения возможных потерь данных и многочасовых простоев в предлагается решить модернизировать существующую серверную инфраструктуру, исключив единую точку отказа и решив проблему быстрого переноса ОС с установленными приложениями с отказавшего сервера на резервный.

Одним из предлагаемых производителями серверов решений является использование блэйд-серверов (серверов-лезвий), размещённых в общем шасси и подключенных к общей дисковой системе хранения данных, что даёт возможность резервному серверу загрузиться из дискового раздела отказавшего сервера. Однако проведённый анализ показал, что такая архитектура эффективна только при большом количестве однотипных серверов с равномерным распределением нагрузки, а в ВС построена вокруг высоконагруженного сервера баз данных, не поддающегося распараллеливанию на несколько физических серверов.

Решение было найдено в виртуализации серверов, обеспечивающей одновременную работу нескольких ОС (виртуальных машин) на одном физическом сервере (хосте). Для упрощения балансировки нагрузки все виртуальные машины были размещены на двух многоядерных серверах, производительности которых достаточно для обеспечения функционирования виртуальных машин, перенесенных с отказавших хостов. Каждый физический сервер снабжен парой контроллеров, подключенных одновременно к двум двухпортовым контроллерам дисковой системы хранения данных IBM DS3512.

В системе хранения используются высокоскоростные накопители на жестких магнитных дисках (НЖМД), каждый из которых оснащён двумя продублированными контроллерами SAS (Serial Attached SCSI). НЖМД объединены в отказоустойчивые дисковые массивы:

- RAID 10, обеспечивающий максимальное быстродействие, – для хранения образов виртуальных машин и баз данных;

- RAID 6, обеспечивающий максимальную ёмкость при сохранении работоспособности в случае отказе двух НЖМД, – для хранения файлового архива.

В результате было реализовано полное дублирование всего аппаратного обеспечения, что, наряду с поддержкой хостами виртуализации динамической многоканальной маршрутизации дискового хранилища, гарантирует сохранение работоспособности серверного кластера при отказе любого контроллера или нарушении контакта в любом разъёме.

Для оперативного устранения возможных сбоев физических серверов они были снабжены контроллерами удалённого администрирования, позволяющими диагностировать и устранять проблемы на этапе загрузки ОС. Средства дистанционного управления дисковой системой хранения данных обеспечивают переназначение доступных серверам дисковых разделов, что в случае отказа сервера позволяет оперативно перенести его виртуальные машины и данные на другой сервер без физического копирования файлов.

Для предотвращения потерь данных вследствие ошибок программистов и администраторов было настроено ежедневное автоматическое резервное копирование на сетевое хранилище данных (NAS), построенное на отказоустойчивом дисковом массиве.

## Заключение

Банки играют огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Благодаря своей специфической роли, со времени своего появления они всегда притягивали преступников. К 90-м годам XX века банки перешли к компьютерной обработке информации, что значительно повысило производительность труда, ускорило расчеты и привело к появлению новых услуг. Однако компьютерные системы, без которых в настоящее время не может обойтись ни один банк, являются также источником совершенно новых угроз, неизвестных ранее. Большинство из них обусловлены новыми информационными технологиями и не являются специфическими исключительно для банков.

Существуют однако два аспекта, выделяющих банки из круга остальных коммерческих систем:

1. Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д.

2. Она затрагивает интересы большого количества организаций и отдельных лиц.

Поэтому информационная безопасность банка — критически важное условие его существования.

В силу этих обстоятельств, к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации. Отечественные банки также не смогут избежать участи тотальной автоматизации по следующим причинам:

- усиления конкуренции между банками;

- необходимости сокращения времени на производство расчетов;

- необходимости улучшать сервис.

Рассмотренные потенциальные опасности и угрозы показывают, что информационная система очень подвержена угрозам со стороны технически грамотных людей. Только постоянное совершенствование подготовки персонала, и грамотная работа с оборудованием могут помочь в защите ценной информаци.

## Список используемой литературы:

1. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2002.

2. Е.Б. Белов, В.П. Лось Основы информационной безопасности. / Москва, Горячая линия – Телеком, 2006

3. Федеральный закон РФ "О персональных данных"

4. Вихорев С.В. Информационная Безопасность Предприятий. Москва, 2006.

5. В.А. Семененко Информационная безопасность. Москва, 2004

6. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков. - Брянск: БГТУ, 2005.

7. Гайкович Ю.В, Першин А.С. Безопасность электронных банковских систем. — М: Единая Европа, 1994 г.

8. Демин В.С. и др. Автоматизированные банковские системы. — М: Менатеп-Информ, 1997 г.

9. Крысин В.А. Безопасность предпринимательской деятельности. — М:Финансы и статистика, 1996 г.

10. Линьков И.И. и др. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. — М: НИТ, 1998 г.

11. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 1997 г.

12. Гайкович В, Першин А. Безопасность электронных банковских систем. - М.,1999.

13. Груздев С. "16 вариантов русской защиты" /КомпьютерПресс №392

14. Груздев С. Электронные ключи. - М. 1993.

15. Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров / /КомпьютерПресс №3, 1995

16. Мафтик С. Механизмы защиты в сетях ЭВМ. /пер. с англ. М.: МИР, 1993.

17. Петров В.А., Пискарев С.А., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. - М., 1998.

18. Спесивцев А.В. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь, 1993.

20. Алексенцев, А.И. Понятие и назначение комплексной системы защиты информации/ А.И.Алексенцев// Вопросы защиты информации.- 1996.- № 2. - С. 2 - 3.

21. Теория информационной безопасности и методология защиты информации: Конспект лекций.

22. Васильевский, А. Защита коммерческой тайны: организационные и юридические аспекты / А.Васильевский [Электронный ресурс]// Valex Consult- (http://www.valex.net/).

23. Мельников Ю.Н., Иванов Д.Ю. Многоуровневая безопасность в корпоративных сетях. Международный форум информатизации - 2000: Доклады международной конференции "Информационные средства и технологии". 17-19 октября 2000 г. В 3-х тт. Т. 2. - М.: Издательство "Станкин", 2000г., - 245 с.

24.Торокин А.А. Основы инженерно-технической защиты информации. - М.: Издательство «Ось-89».1998

|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |

1. Черкасова Е.В., Кирко Е.В. Основы информационной безопасности. [↑](#footnote-ref-1)