МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Проект политики информационной безопасности банка»**

Студент:

Лэ Никита  
Зыонгович

Вариант 8

Преподаватель:

Берников Владислав Олегович

Минск 2020

Содержание

[Введение 3](#_Toc32947952)

[1 Объекты защиты 4](#_Toc32947953)

[1.2 Структура банка 4](#_Toc32947954)

[1.3 Угрозы безопасности информации и их источники 5](#_Toc32947955)

[1.4 Разработка мер защиты 6](#_Toc32947956)

[1.5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 10](#_Toc32947957)

[1.5.1 Формирование политики безопасности 11](#_Toc32947958)

[1.5.2 Регламентация допуска сотрудников к использованию информационных ресурсов 12](#_Toc32947959)

[1.5.3 Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов 13](#_Toc32947960)

[1.5.4 Подбор и подготовка персонала, обучение пользователей 13](#_Toc32947961)

[1.5.5 Подразделение обеспечения информационной безопасности 14](#_Toc32947962)

[1.5.6 Средства обеспечения информационной безопасности Банка 16](#_Toc32947963)

[Вывод 18](#_Toc32947964)

# **Введение**

Репутация кредитного учреждения – нематериальный, но ценный актив. Для того чтобы сохранить доверие клиентов, необходимо обеспечить сохранение банковской и коммерческой тайны. Для оптимального решения этой задачи необходимо разработать политику информационной безопасности банка, которой неукоснительно должны следовать все его служащие.

Деятельность банков Беларуси регулируется ЦБ РБ. Не мог ЦБ остаться в стороне и от обеспечения политики информационной безопасности, поэтому им были предложены банкам стандарты, описывающие рекомендованные методики защиты конфиденциальной информации. Интересно, что в этих стандартах носителем основной угрозы становятся не хакеры или конкуренты, а сотрудники, инсайдеры. В качестве основного источника риска ЦБР видит конфликт между наемным работником и собственником банка, который и приводит к преднамеренным утечкам информации.

Защита документооборота и баз данных хранящих практически всю информацию о клиентах и сотрудниках является сложной, но обязательной задачей, без решения которой невозможно нормальное функционирование банков.

Деятельность банков строго регламентируется, и источником высшей власти в акционерном обществе или обществе с ограниченной ответственностью становится Совет директоров. Именно его одобрение должно лечь в основу разработки политики информационной безопасности.

## **Объекты защиты**

Основными объектами системы информационной безопасности в Банке являются:

* информационные ресурсы с ограниченным доступом, составляющие конфиденциальную информацию, в том числе коммерческую, банковскую тайну, персональные данные или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Банка, независимо от формы и вида ее представления. Информация, находящаяся на файлсерверах, базы данных, носители информации и прочая информация, включая пароли пользователей;
* процессы обработки информации в информационной системе Банка, информационные технологии, регламенты и процедуры сбора, систематизация, накопление, уточнение, использование, хранение, блокирование, уничтожение и передача информации, пользователи и администраторы АБС;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты АБС.

## **1.2 Структура Банка**

Информационная среда Банка является распределенной структурой, объединяющей информационные подсистемы Главного офиса и внутренних структурных подразделений.

К основным особенностям информационной среды Банка относятся:

* широкая территориальная распределенность компонентов информационной системы (Главный офис, Дополнительные офисы и другие внутренние структурные подразделения);
* значительное расширение сферы использования автоматизированных систем обработки информации;
* разнообразие решаемых задач (от подготовки и отправки платежей до внедрения дистанционного банковского обслуживания);
* значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных (подготовка отчетности, подготовка рейсов, отправка денежных переводов и др.);  объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
* абстрагирование владельцев данных от физических структур и места размещения данных (информации);
* наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации) (сеть Интернет и другие специализированные компьютерные сети);
* интенсивность информационных потоков между подразделениями Банка;
* разнообразие категорий доступа обслуживающего персонала к эксплуатируемым системам.

## **1.3 Угрозы безопасности информации и их источники**

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

Искусственные угрозы - это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;
* непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также процедур, правил и требований ИБ и другие действия сотрудников подразделений Банка при эксплуатации АБС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников);

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации Банка являются:

* непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также процедур, правил и требований ИБ и другие действия сотрудников подразделений Банка при эксплуатации АБС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников);
* преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников подразделений Банка, допущенных к работе с АБС Банка, а также сотрудников подразделений Банка, отвечающих за обслуживание и администрирование программного и аппаратного обеспечения, средств защиты и обеспечения ИБ;
* деятельность преступных групп, экономических структур, а также отдельных лиц по добыванию и/или искажению информации, нарушению работоспособности системы в целом или ее отдельных компонентов;
* воздействия из внутренней сети Банка со стороны сотрудников подразделений Банка, а также удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (сети Интернет), используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам Банка;
* нарушение конфиденциальности (разглашение, утечка) сведений, составляющих банковскую или коммерческую тайну, а также персональных данных.
* ошибки, допущенные при проектировании АБС и ее системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) АБС;
* аварии, стихийные бедствия и прочие форс-мажорные обстоятельства.

Наиболее значимыми угрозами безопасности информации Банка (способами нанесения ущерба субъектам информационных отношений) являются:

* нарушение функциональности компонентов информационной системы Банка, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов Банка, а также фальсификация (подделка) документов;
* нарушение конфиденциальности (разглашение, утечка) сведений, составляющих банковскую или коммерческую тайну, а также персональных данных.

Пользователи, операторы и другие сотрудники Банка являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций, регламентов и порядков.

## **1.4 Разработка мер защиты**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Атака | Меры защиты | Ущерб | Вероятность | Риск |
| Кражи, нападения, взлом, саботаж и проникновение | Наличие охраны;  Наличие системы видеонаблюдения;  Наличие пропускной системы с удостоверением личности для рабочего персонала. | 4 | 0,1 | 0,4 |
| Отказы и неисправности технических средств | Наличие отдела, отвечающего за ремонт технических средств | 1 | 0,3 | 0,3 |
| Фарминг | Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение;  Использовать защиту электронного почтового ящика (отключить предварительный просмотр);  Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов. | 1 | 0,2 | 0,2 |
| Mailbombing | Давать адрес электронной почты только проверенным источникам; В качестве преграды для mailbombing-а может выступать и Web-сайт провайдера, иногда настраиваемый таким образом, чтобы он автоматически определял почтовые атаки. Если количество сообщений из одного источника превышает некие разумные пределы, то все они автоматически поступают в Recycle Bin на сервере. | 2 | 0,3 | 0,6 |

Продолжение таблицы на ст. 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Анализатор трафика | Аутентификация - cильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Под "сильным" мы понимаем такой метод аутентификации, который трудно обойти. Примером такой аутентификации являются однократные пароли (OTP - One-Time Passwords);  Коммутируемая инфраструктура - еще одним способом борьбы со сниффингом является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктуры не ликвидирует угрозу сниффинга, но заметно снижает ее остроту;  Антиснифферы как ещё один способ борьбы со сниффингом, который заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в Вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности, они включаются в общую систему защиты.  Криптография - самый эффективный способ борьбы со сниффингом пакетов хотя и не предотвращает перехвата и не распознает работу снифферов, но делает эту работу бесполезной. | 4 | 0,3 | 1.2 |

Продолжение таблицы на ст. 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP-спуфинг | Угрозу спуфинга можно ослабить с помощью:  контроля доступа. Чтобы снизить эффективность IP-спуфинга, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети;  фильтрации RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети. Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. | 4 | 0,3 | 1.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Переполнение буфера | Корректировка исходных кодов программы для устранения уязвимостей. Переполнение буфера происходит, прежде всего, из-за неправильного алгоритма работы программы, который не предусматривает проверок выхода за границы буферов. Также возможно применение специальных утилит автоматического поиска уязвимостей в исходном коде программы.  Использование неисполнимых буферов. Суть метода заключается в запрещении исполнения кода в сегментах данных и стека, т.е. параметры сегментов данных и стека содержат только атрибуты записи и чтения, но не исполнения. Применение проверок выхода за границы. В основе данного метода лежит выполнение проверок выхода за границы переменной при каждом обращении к ней. Это предотвращает все возможные атаки по переполнению буфера, так как полностью исключает само переполнение.  Применение проверок целостности. Решение, получено благодаря проекту Synthetix. Цель Synthetix - специализация кода для увеличения производительности операционных систем. При этом вводится понятие так называемого квази-постоянства (Quasi-invariant), т.е. состояния среды, которое неизменно в определенных рамках. Такое квази-постоянство позволяет устранить ряд избыточного кода проверки выполнения различных условий. | 2 | 0,2 | 0,4 |

Продолжение таблицы на ст. 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отказ в обслуживании (Denial of Service - DoS) | Функции анти-спуфинга - правильная конфигурация функций анти-спуфинга на ваших маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку. Функции анти-DoS - правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени. | 2 | 0,3 | 0,6 |
| Атака типа man-in-the-middle. | Использование шифрования данных | 4 | 0,3 | 1.2 |
| Фишинг | Использовать только проверенные ресурсы и пути доступа к ним;  Использовать антивирусные средства и регулярно обновлять их сигнатуры. | 4 | 0.3 | 1.2 |
| Парольные атаки | Одноразовые пароли;  Криптографическая аутентификация. | 4 | 0.3 | 1.2 |
| Атаки на уровне приложений | Необходимо читать лог – файлы операционных систем и сетевые лог – файлы и/или анализируйте их с помощью специальных приложений;  Пользоваться самыми свежими версиями ОС и приложений и самыми последними коррекционными модулями (патчами); | 4 | 0.2 | 0.8 |

## **1.5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Все меры обеспечения безопасности информационной системы Банка подразделяются на:

* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).

**Законодательные (правовые) меры защиты**

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы Банка.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Банка в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

**Технологические меры защиты**

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений, периодическое подведение общего баланса всех банковских счетов и т.п.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

### **1.5.1 Формирование политики безопасности**

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в Банке целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Банка в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

* каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;
* определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации ограниченного распространения
* кто имеет права доступа к информации ограниченного распространения, кто и при каких условиях может читать и модифицировать информацию и т.д.

Политика нижнего уровня должна:

* предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;
* определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации ограниченного распространения;
* выбирать программно-технические (аппаратные) средства криптозащиты, противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

### **1.5.2 Регламентация допуска сотрудников к использованию информационных ресурсов**

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационной системой Банка и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно, регламента предоставления доступа пользователей.

Основными пользователями информации в Корпоративной информационной системе являются сотрудники структурных подразделений Банка. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

* каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с подразделением Банка, ответственным за информационное сопровождение данного ресурса;
* начальник имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;
* наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники Банка или других организаций, зарегистрированные как легальные пользователи информационной системы Банка и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и коммерческой тайны, а также правил работы с информацией в Банке.

Обработка информации в компонентах информационной системы Банка должна производиться в соответствии с утвержденными технологическими инструкциями.

### **1.5.3 Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов**

Подлежащие защите ресурсы системы (документы, задачи, сервера, программы) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Банка, с которых возможен доступ к ресурсам корпоративной информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей. Все неиспользуемые в работе устройства ввода-вывода информации (COM, LPT, USB, IR порты, дисководы НГМД, CD) на рабочих местах сотрудников, работающих с конфиденциальной информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены. Дополнительные устройства обмена информацией могут использоваться только в исключительных случаях и только в качестве временного средства. Установка подобных устройств должна согласовываться с подразделениями обеспечения информационной безопасности Банка.

В компонентах корпоративной информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться программные средства, только полученные от Управления информационных технологий. Использование программного обеспечения, не прошедшего проверку и не учтенного в Банке, должно быть запрещено.

Для решения специальных задач по оценке защищенности информационной сети Банка и построении системы защиты информации в сети Банка может применяться специальное программное обеспечение, согласованное с Управлением информационных технологий.

### **1.5.4 Подбор и подготовка персонала, обучение пользователей**

Пользователи информационной системы Банка, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в Банке.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Банка. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы Банка, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационной системы Банка должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности Банка, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

### **1.5.5 Подразделение обеспечения информационной безопасности**

Основные функции подразделения обеспечения информационной безопасности заключаются в следующем:

* формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы Банка;
* подготовка решений по обеспечению конфиденциальности, доступности, целостности данных, в том числе решений по обеспечению надежной защиты от мошенничества при использовании пластиковых карт;
* участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;
* обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
* генерация и распределение между пользователями необходимых атрибутов доступа к ресурсам информационной системы Банка;
* наблюдение за функционированием системы защиты и ее элементов;
* проверка надежности функционирования системы защиты;
* разработка мер нейтрализации моделей возможных атак;
* обучение пользователей и обслуживающего персонала правилам безопасной обработки информации;
* оказание методической помощи сотрудникам банка в вопросах обеспечения информационной безопасности;
* контроль за действиями администраторов баз данных, серверов и сетевых устройств;
* контроль за соблюдением пользователями и обслуживающим персоналом
* установленных правил обращения с информацией;
* организация по указанию руководства служебного расследования по фактам нарушения правил обращения с информацией и оборудованием;
* принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;
* cбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

Организационно - правовой статус подразделения обеспечения информационной безопасности Банка должен определяться следующим образом:

* численность подразделения должна быть достаточной для выполнения всех перечисленных выше функций;
* сотрудники, занимающиеся обеспечением информационной безопасности Банка не должны иметь других обязанностей, связанных с обеспечением функционирования технических компонентов информационной системы Банка;
* сотрудники подразделения обеспечения информационной безопасности должны иметь право доступа во все помещения, где, установлены технические средства информационной системы Банка, и право прекращать обработку информации при наличии непосредственной угрозы для нее;
* руководителю подразделения должно быть предоставлено право запрещать включение новых компонентов информационной системы Банка в число действующих, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз безопасности информации;
* подразделению обеспечения информационной безопасности должны обеспечиваться все условия, необходимые для выполнения своих функций.

Для решения задач, возложенных на подразделение обеспечения информационной безопасности, его сотрудники должны иметь следующие права:

* определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы Банка в указанной области;
* получать информацию от пользователей информационной системы Банка по любым аспектам применения информационных технологий в Банке;
* участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
* участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
* контролировать деятельность пользователей информационной системы Банка по вопросам обеспечения информационной безопасности.

В состав подразделения обеспечения информационной безопасности должны входить следующие специалисты:

* ответственные за управление средствами защиты информации (выбор, установка, настройка, снятие средств защиты, просмотр журналов регистрации событий, оперативный контроль, за работой пользователей, и реагирование на события защиты и т.п.);
* ответственные за управление криптографическими средствами защиты (установка, настройка, снятие СКЗИ, генерация и распределение ключей и т.д.);
* ответственные за решение вопросов защиты информации в разрабатываемых и внедряемых в Банке информационных технологиях (участие в разработке технических заданий по вопросам защиты информации, выбор средств и методов защиты, участие в испытаниях новых технологий и программ с целью проверки выполнения требований по защите информации и т.д.);
* специалисты по защите от утечки информации по техническим каналам.

### **1.5.6 Средства обеспечения информационной безопасности Банка**

Для обеспечения информационной безопасности Банка используются следующие средства защиты:

* физические средства (применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации);
* технические средства (меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.));
* средства идентификации и аутентификации пользователей (возможность распознавания каждого легального пользователя);
* средства разграничения доступа (зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства);
* средства обеспечения и контроля целостности (средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных);
* средства оперативного контроля и регистрации событий безопасности (должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение Концепции безопасности и привести к возникновению кризисных ситуаций);
* криптографические средства (использования криптографических методов, является создание инфраструктуры безопасности и использованием открытых ключей (PKI, Public Key Infrastructure)).

Средства защиты должны применяться ко всем чувствительным ресурсам информационной системы Банка, независимо от их вида и формы представления информации в них.

# **Вывод**

Опыт показывает, что для достижения удачных решений по защите информации необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.

Согласно промежуточным результатам исследования, все юридические фирмы имеют незакрытые критические уязвимости на ПК и серверах, половина – на сетевом оборудовании. 65% юрфирм не имеют даже минимальной системы защиты, 60% – уязвимы для действий инсайдеров, а 70% – не защищены от внешних угроз. Причинами подобных цифр, по мнению авторов исследования, являются отсутствие шифрования данных; отсутствие процессов обеспечения безопасности и реагирования на инциденты; неразграничение прав доступа; из всех средств защиты в основном присутствуют только антивирус и слабые пароли. На практике это, в частности, означает высокую вероятность взлома; моментальную доступность конфиденциальной информации при утере или выемке устройства, на которой она хранится; неотслеживаемость действий инсайдеров; невозможность узнать и отреагировать на кибератаку. В частности, нарушение конфиденциальности данных юридической фирмы и их клиентов зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – юридическая фирма понесет ответственность – начиная от финансовой и закачивая уголовной. Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий: четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием; обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия; строгий подбор сотрудников с привлечением, при необходимости, без данных милиции; защита главных серверов компании и важной корпоративной почты; использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов; разграничение доступа к финансовым отделам. проведение регулярных бесед и инструктажей с сотрудниками; наличие в офисе наглядного отображения плана по работе во время чрезвычайных ситуаций. Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.