Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Проект политики информационной безопасности**

для банка

Разработал: Круглик А.В.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Содержание**

[Введение 3](#_Toc126957973)

[Описание структуры банка 5](#_Toc126957974)

[Оценка рисков 7](#_Toc126957975)

[Разработка мер защиты 9](#_Toc126957976)

[Процедурный уровень 9](#_Toc126957977)

[Программно-технический уровень 10](#_Toc126957978)

# **Введение**

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Разработанная и утвержденная документация должна включать в себя следующие разделы:

* перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;
* описания технологий, применяемых для обеспечения сохранности информации;
* перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;
* описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;
* описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;
* описание применяемых организационных мер, действий сотрудников компании по обеспечению информационной безопасности;
* описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;
* описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;
* описание того, в каком порядке будут проводиться аварийные и восстановительные работы при повреждении аппаратной части в случае пожара, проблем с электросвязью или по иным причинам, повлекшим за собой гибель компьютеров, носителей информации или самих баз данных;
* план мероприятий по постоянному поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Целью политики является регламентирование единых подходов и требований по обеспечению информационной безопасности сотрудниками банка, а также организациями, иными юридическими лицами и индивидуальными предпринимателями в рамках оказания им услуг банком.

Достижение указанной цели предполагает решение следующих задач:

* реализация требований законодательства государства в части информационной безопасности информационных систем и мер контроля их защищенности;
* определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности банка;
* своевременное выявление и оценка причин, условий и характера угроз информационной безопасности и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности;
* планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;
* реализация программ по осведомленности и обучению сотрудников (работников) банка о возможных факторах рисков информационной безопасности и мерах противодействия.

# **Описание структуры банка**

Структура банка – это форма организации его внутренних элементов: подразделений, управлений и служб**.**

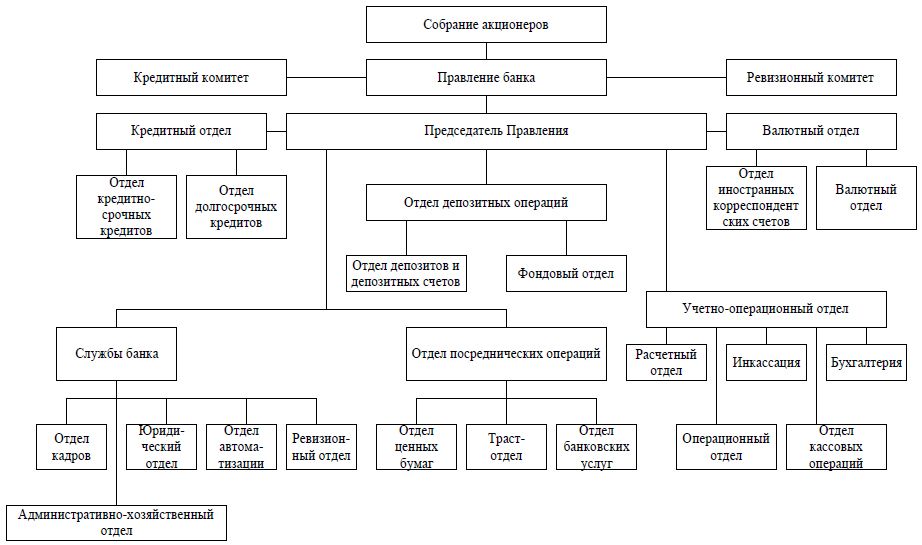


Рисунок 1–Структура банка

Среди внутренних аспектов работы банка особенно важными оказываются:

* Основные направления деятельности: кредитование, привлечение средств во вклады, расчетные и обменные операции, пр.;
* Масштаб деятельности банка: один или несколько близких городов, представительства в регионах страны, международные структуры;
* Важнейшие категории клиентов банка: частные лица, производственные или торговые предприятия, отдельные отрасли и др.

К внешним условиям относятся:

* Указания владельцев банка;
* Цели создания данной конкретной организации;
* Ее место в финансово-экономической системе страны или региона.

В банковской практике стран с развитой рыночной экономикой принята трехступенчатая классификация внектов управления в зависимости от объема их распорядительных полномочий.

Высшее руководство (дирекция) — в его компетенцию входит принятие основополагающих решений по поводу целевых установок и экономической политики банка, подбор и расстановка кад­ров, руководство нижестоящими управленческими подразделениями.

Среднее руководство (руководители отделов) осуществляет управление отдельными сферами банковской деятельности, регулирование процесса работы, руководство подчиненными служащими, подготовку принятия решений для дирекции.

Низшее руководство (руководители групп) распределяет задания и контролирует работу отдельных групп.

Обеспечение безопасности и надёжности объектов информации является одной из основных задач при разработке политики информационной безопасности. В банковской компании можно выделить следующие объекты, требующие обеспечения информационной безопасности:

* технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
* информационные ресурсы, в том числе содержащие сведения ограниченного распространения и представленные в виде документов в носителях на магнитной, оптической и другой основе, массивах и базах данных;
* программные средства (операционные системы, системы управления базами данных и другое программное обеспечение);
* каналы связи, передающие информацию (кабельные и беспроводные, локальные и глобальные каналы связи).

Не менее важным направлением разработки политики информационной безопасности является анализ, характеристика и разработка мер защиты субъектов информационной системы. Далее описаны субъекты, существующие в организации банковской компании:

* сотрудники организации, являющиеся пользователями технологического оборудования, имеющие доступ к информации, размещенной в носителях на магнитной и оптической основе;
* сотрудники отделов и управлений, анализирующие данные в массивах и базах данных;
* пользователи услуг банковской компании, имеющие доступ к информационным ресурсам посредством электронных изданий;
* процессы передачи информации по каналам связи.

# **Основные угрозы и их источники**

Список потенциальных угроз информационным системам банка:

* несанкционированный доступ к базам данных банковской фирмы;
* модификация программного обеспечения банковских терминалов, информационно-справочных систем банка;
* модификация процедур осуществления денежных транзакций, терминалов безналичного расчёта;
* различного рода атаки на банковские серверы;
* несанкционированный доступ банковским архивам документов и т.д.

Потенциальные угрозы также можно классифицировать по природе их возникновения: естественные и искусственные.

Естественные угрозы – это угрозы, вызванные объективными физическими процессами техногенного характера, или стихийными природными явлениями, которые не зависят от деятельности человека.

К естественным угрозам в банковской компании можно отнести внешние климатические условия, перебои в электроснабжении, а также электрические, магнитные, электромагнитные и ионизирующие помехи.

Искусственные угрозы отличаются от естественных тем, что они вызваны деятельностью человека. К искусственным угрозам можно отнести следующие вышеописанные потенциальные угрозы:

* несанкционированный доступ к базам данных, программным средствам и прочим документам третьими лицами и сотрудниками банковской компании;
* доступ к базам данных, программным средствам и прочим документам сотрудниками, не обладающими достаточной квалификацией;
* заражения компьютерных систем компании компьютерными вирусами;

Помимо вышеперечисленных классификаций потенциальных угроз, угрозы информационной безопасности также можно разделить по степени умысла на преднамеренные и непреднамеренные.

Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) угрозы – это угрозы, к которым относятся непреднамеренные нарушения правил сбора, обработки и передачи информации, а также случайные нарушения требований безопасности и другие действия сотрудников банковской компании, приводящие к непроизводительным затратам времени и ресурсов, разглашению личной информации клиентов компании или конфиденциальной информации компании, потере важных данных или нарушению работоспособности банковской компании.

Все непреднамеренные угрозы можно отнести к человеческому фактору. Человеческий фактор – это совокупность характеристик человека, которые свидетельствуют о его надёжности и производительности в определённых ситуациях. На это влияют многие факторы, такие как возраст, душевное состояние, физическое здоровье, эмоции, склонность к определенным распространенным ошибкам, когнитивным заблуждениям и т.д.

В качестве примеров непреднамеренных угроз в банковской компании можно привести:

* профессиональные ошибки сотрудников банковской компании из-за излишней самоуверенности, недостатка знаний или случайностей;
* нарушения целостности и безопасности баз данных, программных средств и прочих информационных средств ввиду случайных ошибок сотрудников;
* непреднамеренные ошибки, нарушения правил эксплуатации, стандартов безопасности, трудовой дисциплины, а также некачественное исполнение обязанностей сотрудников ввиду следующих факторов: психоэмоционального и физического состояния, проблемах в межличностных отношениях, конфликтах на работе и прочих непреднамеренных форс-мажорных обстоятельств.

Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) угрозы – это угрозы, обусловленные осмысленными корыстными действиями легально допущенных к информации сотрудников банковской компании, приводящие к непроизводительным затратам времени и ресурсов,

разглашению личной информации клиентов компании или конфиденциальной информации компании, потере важных данных или нарушению работоспособности банковской компании.

К данному типу угроз относятся все виды влияния человеческого фактора, которые обусловлены злым умыслом либо некачественным или неквалифицированным исполнением обязанностей.

К преднамеренным угрозам и ошибкам относятся все правонарушения против безопасности, нарушения трудовой дисциплины, конфликты, кражи и т.д. В этих случаях у человека есть вина, мотив, осознание действия и он, как правило, имеет чёткое представление о том, что произойдёт в случае обнаружения его ошибки, или же он точно знает, что его лень, халатность или недопонимание рано или поздно приведут к ошибке.

К преднамеренным угрозам в банковской компании можно отнести:

* удаленный несанкционированный доступ третьих лиц или сотрудников компании к информационным ресурсам банковской компании с целью получения материальной выгоды;
* неправомерный доступ к ресурсам компании ранее уволенными сотрудниками, который может повлечь утечку данных компаниям-конкурентам;
* физическое неправомерное нарушение целостности средств хранения важных информационных источников техногенного и естественного характера третьими лицами путём взлома, краж.

Внутренние дестабилизирующие факторы влияют:

На программные средства (ПС):

* некорректный исходный алгоритм;
* неправильно запрограммированный исходный алгоритм.

На аппаратные средства (АС):

* системные ошибки при постановке задачи проектирования;
* отклонения от технологии изготовления комплектующих изделий и аппаратных средств в целом;
* нарушение режима эксплуатации, вызванное внутренним состоянием АС.

К конкретным внутренним угрозам, которые имеют место в банковской компании, можно отнести:

* нарушения в работе алгоритмов используемых в работе программных средств, а также нарушение эксплуатации используемых аппаратных средств;
* системные ошибки в технологическом оборудовании, которые могут привести к уничтожению критически важных данных;
* внутренние ошибки в клиентских базах данных, которые могут привести к искажению и уничтожению пользовательских данных.

Внутренние угрозы не являются высоковероятными вследствие развития технической аппаратуры, однако, при своей реализации внутренние угрозы могут нанести существенный ущерб для банковской компании.

Внешние дестабилизирующие факторы влияют:

На программные средства (ПС):

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода.

На аппаратные средства (АС):

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* недостаточная квалификация обслуживающего персонала.

Рассмотрим конкретные внешние дестабилизирующие факторы, которые имеют риски реализации в банковской компании:

* несанкционированный доступ к базам данных, программным средствам и прочим документам третьими лицами, который может повлечь искажение, потерю и утечку личных данных пользователей и конфиденциальных данных банковской компании;
* несанкционированный доступ к базам данных, программным средствам и прочим документам сотрудниками банковской компании, не имеющих привилегий на доступ к этим данным;
* доступ к данным сотрудниками банковской компании, не обладающих достаточной квалификацией;
* заражения компьютерных систем компании компьютерными вирусами, которые могут причинить ущерб в виде блокировки доступа или уничтожения файлов, а также передачи информации третьим лицам;
* человеческий фактор.

Внешние угрозы являются гораздо более высоковероятными и также могут нанести серьёзный ущерб, поэтому вследствие их высоких рисков они должны классифицироваться в политике информационной безопасности, и требуют разработки методов и средств обеспечения требуемого уровня защищённости информационной системы.

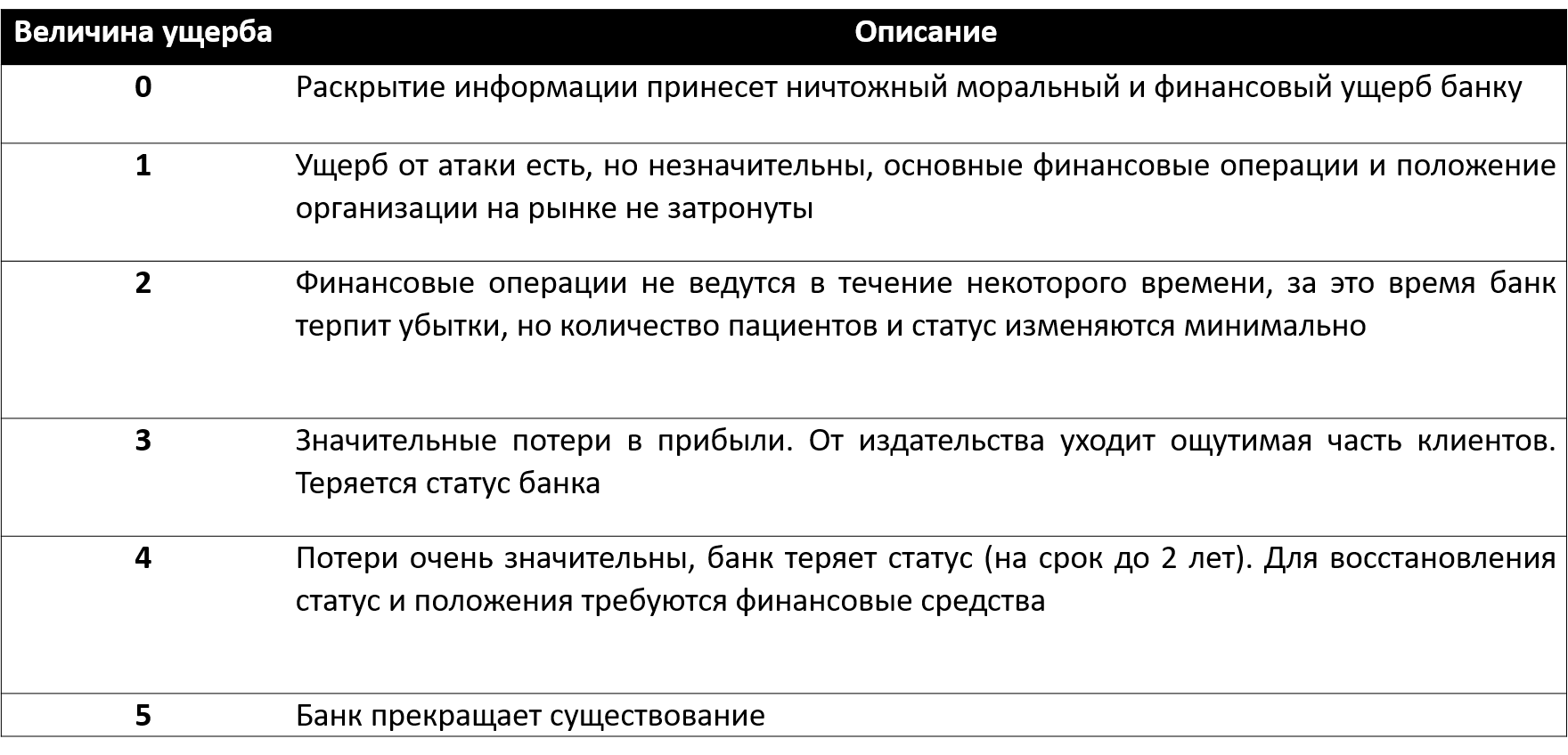
# **Оценка рисков**

Ценность информационных ресурсов банка характеризуется возможным вредом финансовому положению банковской фирмы, а также понижением её репутационных характеристик. Особой ценностью обладают информационных объекты, содержащие информацию о клиентах банка, их счетах и проводимых между ними операциях. Не меньшей ценностью обладают договоры, ценные бумаги, расписки, их бумажные и электронные копии.

Значимость определённых угроз зависит от вреда, которые они могут нанести информационным системам и банковской компании в целом. Примеры угроз:

* нарушение целостность информации, хранящейся на банковских серверах;
* получения доступа к информации третьими лицами;
* обнародование секретной или конфиденциальной информации;
* несанкционированный доступ к помещениям, содержащим ценные бумаги и документы;

Таблица 1– Численная шкала для оценки ущерба



Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

Оценка эффективности существующих или планируемых средств защиты основывается на глубоком анализе истории неблагоприятных для информационной системы банка ситуаций: возникновение серверных атак, конфликтных ситуаций с клиентами, возникших на основе нарушения целостности банковской информации и получения третьими лицами доступа к конфиденциальной информации и т.д.

Чтобы определить вероятность выполнения одного из критических сценариев развития, угрожающих целостности информационной системе, ситуаций необходимо оценить привлекательность информационного ресурса как показателя при рассмотрении угрозы от умышленного воздействия со стороны человека:

* ценные бумаги, документы – высокая ценность;
* справочная информация, база данных клиентской информации – средняя ценность;
* информация о проведённых транзакциях по счетам – средняя, низкая ценность.

Оценка рисков предполагает анализ средств, при помощи которых злоумышленник может навредить информационной системе банка, или стихийных бедствий, который могут сдать причиной уничтожения физических носителей информации:

* специально ПО для доступа к банковским серверам;
* вирусы, «трояны», «черви» и другое вредоносное программное обеспечение, способные нанести вред банковскому ПО и информационным системам;
* средства взлома сигнализации и различных других защитных систем здания банка;
* ПО для подбора паролей и взлома защищённых информационных объектов и т.д.

Таблица 2 – Оценка рисков



# **Разработка мер защиты**

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях.

# **Процедурный уровень**

Можно выделить следующие группы процедурных мер:

* управление персоналом:

1. для каждой должности существуют квалификационные требования по информационной безопасности. Таким образом, необходимо ограничить доступ и предоставить достаточно высокий уровень доступа определённым работникам банка. Работники банка, которым предоставлен высший уровень доступа к ценным бумагам, документам, базам данных и серверным должны быть должным образом проинструктированы о политике информационной безопасности банка и быть готовы реагировать на внештатные ситуации в соответсвии с распорядком;
2. весь рабочий персонал должен быть проинструктирован о возможных угрозах информационной безопасности банка;
3. каждый работник должен изучить меры безопасности теоретически и на практике;
4. отдельным работникам доступ к важным бумагам и информационным объектам должен быть ограничен;

* физическая защита:

1. установка охранных и охранно-пожарных систем в здании банка;
2. установка средств охранного телевидения: камеры, экраны наблюдения, зеркальные щиты и т.д.;
3. установка охранного освещения;
4. установка, где присутствует необходимость, ограждений и физической изоляции;
5. установка запирающих устройств на дверные проёмы и двери;
6. установка систем контроля доступа: карты доступа, средства опознавания по отпечаткам пальцев, голосу, почерку, геометрии рук;
7. установка радиолучевых, радиоволновых и инфракрасных защитных систем: антенн, глушителей и т.д.

* поддержание работоспособности:

1. проведение своевременных ревизий защитного оборудования банка;
2. ежедневный контроль исправности защитного оборудования;

* реагирование на нарушения режима безопасности:

1. необходимо назначить несколько рабочих лиц, отвественных за безопасность информационной системы банка;
2. разделение локальных сетей банка на сегменты и своевременной их отключение;
3. необходимо стремится к скорейшей локализации инцидента и выявлению нарушителя;
4. активизация всех защитных систем банка и блокировка доступа ко всем объектам информационной системы банка;

* планирование восстановительных работ:

1. разработка стратегий восстановительных работ;
2. определение перечня возможных аварий;
3. обеспечение информационной системы банка избыточными мерами резервного копирования, хранения копий информации и представления информации в разных видах;
4. заключение соглашений с поставщиками информационных услуг по защите информации;
5. проверка и практическая реализация стратегии восстановительных работ;
6. определение средств штатной работы банка в случае критической ситуации и прорабатывание с персоналом банка сценариев развития внештатных ситуаций.

# **Программно-технический уровень**

Основой программно-технического уровняявляются следующие механизмы безопасности:

* идентификация и аутентификация пользователей:

1. установка средств идентификации/аутентификации пользователей (паролей, средств двухфакторной аутентификацией и т.д.);
2. предоставление необходимости подтвердить свою личность в случае подозрительной деятельности пользователя;
3. предоставление необходимости смены пароля или иных средств идентификации/аутентификации в случае длительного их использования или подозрительной деятельности пользователя;

* управление доступом:

1. предоставление работникам банка средств контроля доступа за деятельностью пользователей;
2. ограничение доступа к отдельным составляющим информационной системы для отдельных пользователей;
3. полное ограничение и предоставление необходимости в подтверждении прав доступа для пользователей, проявляющих подозрительную активность;

* протоколирование и аудит:

1. контроль за действиями пользователя во время пользования информационной системой;
2. протоколирование и ревизия действий пользователей;
3. постоянный аудит работоспособности защитных устройств и систем отдельных информационных объектов;
4. проведение анализа защищённости объектов и процедур по проверке отказоустойчивости защитных систем;

криптография:

1. обеспечение надёжных систем шифрования данных;
2. постоянная разработка и модификация алгоритмов шифрования;
3. аудит секретности шифровальных систем и защищённости алгоритмов шифрования от несанкционированного доступа;

* экранирование:

1. установка средств экранирования информационных каналов;
2. мониторинг информационных систем на факт наличия источников утечки информации;
3. установка телекоммуникационных и электроакустических систем экранирования;
4. установка защитного антивирусного программного обеспечения на объекты информационной системы банка.

* обеспечение высокой доступности:

1. структуризация элементов информационной системы;
2. апробирование всех процессов и составных частей информационной системы;
3. автоматизация процессов информационной системы;
4. обеспечение модульности архитектуры информационной системы;
5. ориентация на простоту решений при разработке архитектуры информационной системы.

**Выводы**

Правильное составление содержания политики информационной безопасности является важным аспектом построения успешной и защищённой компании. Политика информационной безопасности компании содержит основные и базовые инструкции по установке, регулированию и контролю защитных средств.

Политика информационной безопасности помогает основательно подготовить фирму к непредвиденным ситуациям и быстро решить возникшую проблему. Также, она содержит инструкции по информационной безопасности для рабочего персонала банка и может использоваться как пособие для консультации работников банка по вопросам данной сферы.

Политика информационной безопасности является одним из звеньев в последовательном ряде решений информационной безопасности, указанное обстоятельство гарантирует должностным лицам банка, что система информационной безопасности, построенная в соответствии с концепцией, будет управляемой, экономически обоснованной и соответствующей требованиям бизнеса.