Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности банка

Студент: Станчик М. А.

ФИТ 3 курс 4 группа

Преподаватель: Савельева М. Г.

Минск 2025

**Содержание**

[ВВЕДЕНИЕ 3](#_Toc127230212)

[1 Объекты защиты 4](#_Toc127230213)

[1.1 Описание структуры организации 4](#_Toc127230214)

[1.2 Внутренняя структура организации 4](#_Toc127230215)

[1.3 Обзор объектов и субъектов информационных отношений 6](#_Toc127230216)

[1.3.1 Объекты информационных отношений 6](#_Toc127230217)

[1.3.2 Субъекты информационных отношений 6](#_Toc127230218)

[2 Основные угрозы и их источники 7](#_Toc127230219)

[2.1 Внутренние угрозы 7](#_Toc127230220)

[2.2 Внешние угрозы 8](#_Toc127230221)

[2.3 Естественные угрозы 8](#_Toc127230222)

[2.4 Искусственные угрозы 9](#_Toc127230223)

[2.5 Непреднамеренные угрозы 9](#_Toc127230224)

[2.6 Преднамеренные угрозы 10](#_Toc127230225)

[3 Оценка угроз, рисков и уязвимостей 11](#_Toc127230226)

[3.1 Оценка ущерба организации 11](#_Toc127230227)

[3.2 Оценка вероятности реализации угроз 12](#_Toc127230228)

[3.3 Оценка рисков 12](#_Toc127230229)

[4 Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов 14](#_Toc127230230)

[4.1 Реализация средств защиты 14](#_Toc127230231)

[4.1.1 Несанкционированный доступ сотрудников 14](#_Toc127230232)

[4.1.2 Санкционированный доступ сотрудников 15](#_Toc127230233)

[4.1.3 Несанкционированный доступ хакеров и их группировок 15](#_Toc127230234)

[4.1.4 Проникновение третьих лиц на рабочие места 16](#_Toc127230235)

[4.1.5 Человеческий фактор 16](#_Toc127230236)

[4.2 Программа обеспечения информационной безопасности 17](#_Toc127230237)

[ЗАКЛЮЧЕНИЕ 18](#_Toc127230238)

# 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 сотрудники.

Политика информационной безопасности – это совокупность правил, процедур, методов, принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации в своей деятельности.

В банковской сфере разработка и внедрение политики информационной безопасности являются критически важными для обеспечения стабильной работы организации. Банки обрабатывают огромные объёмы конфиденциальной информации, включая персональные данные клиентов, такие как номера счетов, паспортные данные, данные кредитных карт, а также финансовую информацию, связанную с операциями и транзакциями. Утечка, искажение, блокировка доступа или уничтожение этих данных могут привести к серьёзным финансовым потерям, утрате доверия клиентов и репутационным рискам для банка. Поэтому обеспечение защиты информации является неотъемлемой частью стратегии развития банка и его устойчивости к атакам.

В связи с этим можно выделить следующие цели и задачи разработки политики информационной безопасности:

Цель: защита информационной среды банка от вмешательства и несанкционированного доступа посторонних лиц, а также от утечки данных через технические каналы.

Основные пути достижения поставленных целей:

* ведение строгого учета всех компонентов информационной системы всех ресурсов, начиная от каждого документа и заканчивая серверами и каналами связи;
* контроль над действиями сотрудников, обеспечивающих обслуживание элементов системы, работающих с программными средствами, осуществляющими резервное копирование, их учет в электронных журналах, позволяющих установить, кто конкретно посещал отдельные информационные ресурсы;
* подготовка всех сотрудников, ответственных за сохранение информационной безопасности, по современным стандартам работы с безопасностью;
* предоставление каждому отдельному сотруднику минимально необходимого объема полномочий по доступу к информационным ресурсам, требуемого для выполнения им своих обязанностей; расширение этого доступа только на основании мотивированных служебных записок, согласованных с руководством банка;
* возложение на каждого сотрудника персональной ответственности за работоспособность системы и защиту информации, привлечение к дисциплинарной и уголовной ответственности в случае ее намеренного разглашения;
* применение программных и технических средств, обеспечивающих работу системы, и непрерывный аудит качества их работы;
* контроль над деятельностью каждого сотрудника, работающего с информационными ресурсами;
* юридическая защита интересов банка в отношениях с третьими лицами, запрашивающими информацию или предоставляющими ее;
* выбор необходимых путей возлагается на руководство банка и департамента информационной безопасности.

# Объекты защиты

# 1.1 Описание структуры организации

Кредитная организация для выполнения своих функций должна быть упорядочена, т.е. иметь такое построение, которое позволит в соответствии со стратегическими целями деятельности банка эффективно координировать использование финансовых, трудовых, материальных и информационных ресурсов.

Высшее руководство банком – собрание учредителей, другая подобная структура. Непосредственным управлением операциями этот орган не занимается, но назначает исполнительные органы и контролирует их деятельность.

Правление банка во главе с председателем – это уже элемент текущего, оперативного управления. В его подчинении находятся руководители всех прочих подразделений.

Управление розничного бизнеса – сюда входят отделы, обслуживающие частных лиц: кредитование, валютно-обменные операции, прием вкладов, операции с банковскими картами и пр.

Управление корпоративного бизнеса – тут речь идет о работе с организациями. Это также кредитование, привлечение средств, производство платежей и прочих расчетов, привлечение средств организаций на депозиты.

Управление безопасности и контроля – отделы с такими задачами могут входить в состав двух приведенных выше управлений или иметь единое руководство. Часто контроль, внутреннюю и внешнюю безопасность разделяют между несколькими отдельными управлениями.

Управление межбанковских коммуникаций – такое подразделение можно считать необходимым на современном этапе консолидации банковской системы. Для работы с банками-партнерами, конкурентами и всеми прочими кредитными учреждениями создается особое управление, либо эти функции остаются в ведении руководства банка.

Бухгалтерия – структура обязательная для любого хозяйствующего субъекта, и всегда имеющая единое руководство.

Управление операций на фондовом рынке – в распоряжении банков, на разных условиях, оказываются ценные бумаги многих предприятий и государств. Для обращения с этими активами банки могут формировать специальные службы.

Юридическое управление – существует во всех банках, имеет в своем названии указание на специализацию и единое руководство.

Управление развития – сюда относятся элементы системы связанные с поиском новых рынков, клиентов, направлений и способов дохода. Отделы развития создаются при разных управлениях или объединяются в единую службу при тесном взаимодействии с другими подразделениями.

Пиар (PR) и реклама – эти направления могут выделяться в отдельные банковские структуры, могут объединяться с управлением развития, или подчиняться подразделениям, ориентированным на определенных клиентов.

Управление информационных технологий – по мере компьютеризации систем обработки информации и развитием удаленного управления, подобные службы стали обязательной частью любой банковской структуры. Они взаимодействуют со всеми отделами, но обычно составляют единую систему.

Региональные подразделения – такие элементы присущи крупным банкам. Система управления в них варьируется по нескольким критериям. Иногда региональные подразделения дублируют в своем составе все перечисленные выше управления и службы, иногда курируют только некоторые направления, к примеру – работу с физическими лицами.

Отраслевые управления – создаются не всегда, но могут быть необходимы банкам, имеющим особые интересы в определенных отраслях или массового потребителя в одной сфере деятельности: сельском хозяйстве, международной торговле, энергетике и др.

Структура коммерческого банка представлена на рисунке 1.1.

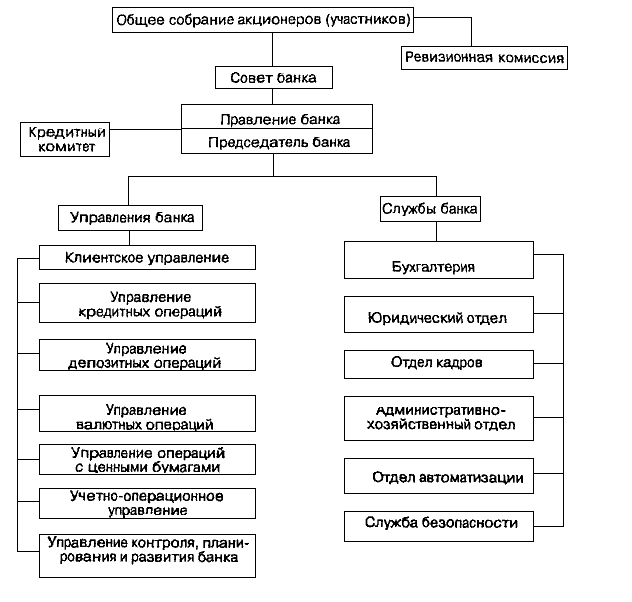


Рисунок 1.1 – Структура коммерческого банка

# Внутренняя структура ИВС

Информационно-вычислительная система (ИВС) коммерческого банка – это комплекс аппаратных и программных средств, а также организационных процессов, предназначенных для обработки, хранения, передачи и защиты информации, связанной с банковскими операциями. ИВС обеспечивает автоматизацию бизнес-процессов и поддерживает основные функции банка, включая финансовые операции, клиентский сервис, управление рисками и соблюдение нормативных требований.

Аппаратные компоненты:

* контроль над деятельностью каждого сотрудника, работающего с информационными ресурсами;
* серверы (основные вычислительные мощности, на которых размещаются базы данных, приложения и системы. Серверы могут быть физическими или виртуальными и обеспечивают выполнение операций и обработку данных);
* системы хранения данных (устройства и решения для хранения больших объемов информации, включая базы данных клиентов, транзакции и отчеты);
* сетевое оборудование (коммутаторы, маршрутизаторы и точки доступа, обеспечивающие связь между различными компонентами системы и доступ к интернету);
* рабочие станции и терминалы (устройства, с помощью которых сотрудники банка получают доступ к ИВС для выполнения своих задач).

Программные компоненты:

* операционные системы (программное обеспечение, обеспечивающее функционирование серверов и рабочих станций);
* базы данных (системы управления базами данных (СУБД) для хранения и управления данными клиентов и транзакциями);
* банковские приложения (программное обеспечение для выполнения различных банковских операций, включая кредитование, расчет процентов, обработку платежей и управление счетами);
* системы безопасности (программные решения для защиты информации от несанкционированного доступа, включая антивирусные программы, системы обнаружения вторжений (IDS) и средства шифрования данных).

Сетевые компоненты:

* локальная сеть (сеть, объединяющая все устройства внутри банка, позволяющая сотрудникам обмениваться данными и получать доступ к ИВС);
* виртуальные частные сети (VPN) (используются для безопасного доступа удаленных сотрудников и филиалов к основным системам банка);
* интернет-соединение (обеспечивает доступ клиентов к онлайн-услугам банка, таким как интернет-банк).

Функции ИВС коммерческого банка:

* обеспечение надежной и быстрой обработки всех финансовых операций, включая переводы, платежи и кредиты;
* автоматизация расчетов и ведение учета всех операций в реальном времени;
* хранение и обработка информации о клиентах, включая личные данные, историю транзакций и кредитные истории;
* сбор и анализ данных для создания отчетов о финансовых показателях, рисках и эффективности бизнеса;
* поддержка принятия управленческих решений на основе анализа данных;
* оценка и управление кредитными, операционными и рыночными рисками с использованием специализированного программного обеспечения;
* реализация механизмов контроля за соблюдением нормативных требований и стандартов;
* защита информации от несанкционированного доступа и киберугроз с помощью многоуровневых систем безопасности;
* регулярные аудиты и тестирование на уязвимости для обеспечения надежности системы;
* обеспечение онлайн-банкинга и мобильных приложений для клиентов, позволяющих им управлять своими счетами, совершать платежи и получать консультации;
* организация службы поддержки для решения вопросов клиентов и обработки запросов.

# Обзор объектов и субъектов информационных отношений

В этом разделе мы проанализируем ключевые объекты и субъекты информационных отношений, защиту которых необходимо обеспечить посредством принятия мер по обеспечению информационной безопасности.

В системе объект выступает в роли пассивного элемента, отвечающего за хранение, обработку, передачу или прием информации. К таким объектам относятся страницы, файлы, папки, директории, компьютерные программы, а также устройства, такие как мониторы, диски, принтеры и прочие.

Активным элементом системы, способным запускать поток информации, выступает субъект. К субъектам относятся пользователь, процесс или устройство.

# Объекты информационных отношений

Защита и надёжность объектов информации выступают в качестве ключевой задачи при создании политики информационной безопасности. В коммерческом банке можно выделить следующие объекты, требующие обеспечения информационной безопасности:

* клиентские данные (личные и финансовые сведения клиентов, включая номера счетов, адреса, телефонные номера и другую конфиденциальную информацию);
* финансовые транзакции (информация о проводимых операциях, включая переводы, платежи и другие финансовые действия);
* банковские системы и приложения (программное обеспечение, используемое для обработки транзакций, управления счетами и предоставления услуг клиентам);
* сетевые инфраструктуры (аппаратные и программные средства, обеспечивающие связь и данные между различными системами и пользователями);
* документы и отчеты (внутренние документы, отчеты о деятельности банка, бизнес-планы и другие важные материалы);
* системы аутентификации и авторизации (механизмы, обеспечивающие доступ к информации и системам только уполномоченным пользователям);
* резервные копии данных (хранение копий критически важной информации для восстановления в случае утраты или повреждения данных);
* физические объекты (помещения, серверы и устройства, на которых хранятся и обрабатываются данные);
* персональные данные сотрудников коммерческого банка;
* партнерские системы (информационные системы третьих сторон, с которыми банк взаимодействует, включая поставщиков и партнеров).

# Субъекты информационных отношений

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

* клиенты (физические и юридические лица, использующие банковские услуги, такие как открытие счетов, получение кредитов и проведение платежей.);
* сотрудники (работники банка, включая кассиров, менеджеров и IT-специалистов, которые осуществляют операции и обеспечивают функционирование банка);
* руководство (высшее руководство банка, принимающее стратегические решения и обеспечивающее соблюдение всех норм и стандартов безопасности);
* аукционеры (лица или организации, владеющие акциями банка и имеющие право голоса на собраниях);
* регуляторы (государственные органы, контролирующие деятельность банков и обеспечивающие соблюдение нормативных актов);
* партнеры (компании и организации, с которыми банк сотрудничает, включая страховые и инвестиционные фирмы);
* аудиторы (внешние и внутренние специалисты, проверяющие финансовую отчетность и эффективность системы безопасности);
* поставщики (компании, предоставляющие технологии и услуги, такие как программное обеспечение и оборудование).

Каждый из этих субъектов играет важную роль в функционировании банка, и разработка мер защиты для них поможет обеспечить комплексную безопасность информационной системы.

# 2 Основные угрозы и их источники

Главной целью разработки политики информационной безопасности является классификация всех возможных типов потенциальных угроз, а также оценка рисков реализации данных угроз. На основании этих данных разрабатываются средства и методы для эффективного управления информационной безопасностью в банке.

Угрозы безопасности могут быть внешнего и внутреннего, искусственного и естественного, а также преднамеренного и непреднамеренного происхождения.

Кроме того, не исключен риск заражения компьютерных систем банка различными вирусами, которые могут причинить существенный ущерб в виде блокировки доступа и уничтожения важных файлов и передачи информации третьим лицам.

Далее будут подробнее рассмотрены основные типы, по которым можно классифицировать потенциальные угрозы.

# Внутренние источники угроз

Внутренние дестабилизирующие факторы влияют:

На программные средства (ПС):

* разработчики;
* администраторы баз данных;
* тестировщики;
* менеджеры проектов.

На аппаратные средства (АС):

* операторы;
* технические специалисты;
* сотрудники, ответственные за закупки.

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

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

Источники угроз:

* человеческий фактор (ошибки сотрудников, как преднамеренные, так и непреднамеренные, могут привести к сбоям в работе как программных, так и аппаратных средств);
* технические недостатки (устаревшее или некорректно настроенное программное обеспечение и оборудование могут стать источником угроз);
* процессы проектирования (неправильная постановка задач и проектирование могут привести к системным ошибкам и сбоям).

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

# Внешние угрозы

Внешние дестабилизирующие факторы влияют:

На программные средства (ПС):

* хактивисты;
* конкуренты;
* поставщики ПО.

На аппаратные средства (АС):

* природные факторы;
* поставщики оборудования.

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

* 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 банка;
* несанкционированный доступ к базам данных, программным средствам и прочим документам сотрудниками банка, не имеющих привилегий на доступ к этим данным;
* доступ к данным сотрудниками банка, не обладающих достаточной квалификацией;
* заражения компьютерных систем банка 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.

# Естественные угрозы

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 банке можно отнести внешние климатические условия, непреднамеренные перебои в электроснабжении, а также электрические, магнитные, электромагнитные и ионизирующие помехи.

# Искусственные угрозы

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 (преднамеренная угроза);
* доступ к базам данных, программным средствам и прочим документам сотрудниками, не обладающими достаточной квалификацией (непреднамеренная угроза);
* заражения компьютерных систем банка компьютерными вирусами (преднамеренная угроза);
* человеческий фактор (преднамеренная угроза).

Если сравнивать между собой естественные и искусственные угрозы, то оба типа угроз могут понести серьезный ущерб и убытки банка, однако, ввиду того, что искусственные угрозы являются гораздо более распространёнными и высоковероятными, их риск становится гораздо выше.

# Непреднамеренные угрозы

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

Непреднамеренные угрозы (ошибочные, случайные, без злого умысла и корыстных целей) включают в себя нарушения правил сбора, обработки и передачи информации, а также случайные нарушения требований безопасности. Эти угрозы могут возникать из-за действий сотрудников банка и приводить к неэффективным затратам времени и ресурсов, разглашению личной информации клиентов или конфиденциальных данных, потере важных сведений и нарушению работоспособности коммерческого банка.

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.

Непреднамеренные угрозы в банке:

* профессиональные ошибки сотрудников банка 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;
* непреднамеренные технические сбои, вызванные ошибками в программном обеспечении или аппаратных средствах, которые могут привести к остановке работы или потере данных;
* неполная или устаревшая документация может привести к неверному пониманию процессов и стандартов, что в свою очередь вызовет ошибки;
* непредусмотренные ситуации, такие как сбой оборудования или программного обеспечения, могут привести к потере критически важных данных из-за отсутствия резервных копий.

# Преднамеренные угрозы

Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом) угрозы – это угрозы, обусловленные осмысленными корыстными действиями легально допущенных к информации сотрудников банка, приводящие к непроизводительным затратам времени и ресурсов, разглашению личной информации клиентов банка или конфиденциальной информации компании, потере важных данных или нарушению работоспособности банка.

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. 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 приведут к ошибке.

К преднамеренным угрозам в коммерческом банке относятся:

* удаленный несанкционированный доступ третьих лиц или сотрудников к информационным ресурсам банка с целью получения материальной выгоды;
* неправомерный доступ к ресурсам банка ранее уволенными сотрудниками, который может повлечь утечку данных банкам-конкурентам;
* халатность сотрудников и невыполнение поставленных обязательств;
* физическое неправомерное нарушение целостности средств хранения важных информационных источников техногенного и естественного характера третьими лицами путём взлома, краж;
* неправильно реализованные программные процессы, вызванные злонамеренными действиями сотрудников или внешних злоумышленников (сотрудники и злоумышленники);
* нарушения в работе программных средств, которые могут быть вызваны целенаправленным вмешательством;
* умышленное повреждение оборудования или его компонентов;
* нарушение эксплуатации аппаратных средств, вызванное действиями сотрудников.

# 3 Оценка угроз, рисков и уязвимостей

Следующим этапом разработки политики информационной безопасности является оценка рисков. Риски можно представить, как совокупность двух факторов: произведения ущерба от реализации угрозы и вероятности её реализации.

Также при оценивании рисков учитываются ценность ресурсов, значимость угроз и эффективность существующих и планируемых средств и методов защиты. Ценность ресурсов может определяться количественной или качественной характеристикой, или их комбинацией.

На основании величины рисков определяются наиболее важные и приоритетные угрозы, и на основании того, какие именно угрозы являются самыми рискованными и критически важными, определяются наиболее приоритетные меры, методы и средства защиты информационных ресурсов, а также необходимые средства управления информационной безопасностью.

То есть, для оценки рисков необходимо создать шкалу оценки ущерба банка, вероятностно-временную шкалу реализации угрозы, которые будут рассмотрены далее.

# 3.1 Оценка ущерба организации

Для оценки возможного ущерба банка от реализации потенциальных угроз составляется таблица численной оценки ущерба организации, где каждой качественной степени ущерба соответствует целочисленное значение от 0 до 5. Благодаря численному ранжированию величины ущерба возможно просчитать риски на каждый тип потенциальной угрозы. Численные оценки ущерба организации представлены в таблице 3.1.

Таблица 3.1 – Численная шкала оценки ущерба коммерческого банка

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб коммерческому банку |
| 1 | Ущерб от атаки есть, но он незначителен, и положение банка на рынке не затронуто |
| 2 | Операции банка не ведутся в течение некоторого времени, банк терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери финансов и доверия со стороны клиентов, ощутимая часть которых уходит |
| 4 | Потери очень значительные, банк на период до года теряет свое положение на рынке. Для восстановления потребуются крупные финансовые займы |
| 5 | Банк прекращает существование |

# 3.2 Оценка вероятности реализации угроз

Кроме того, чтобы оценить величину ущерба от реализации каждой потенциальной угрозы информационной безопасности коммерческого банка, необходимо также учитывать вероятность того, что данная угроза вообще будет реализована. Эта вероятность обусловлена следующими факторами:

* уровень защиты информации: эффективность текущих систем безопасности, включая программное обеспечение, аппаратные средства и процедуры;
* уязвимости системы: наличие слабых мест в информационных системах, которые могут быть использованы злоумышленниками;
* история инцидентов: анализ предыдущих случаев мошенничества или атак на банк, которые могут указывать на вероятность повторения;
* технические тренды: развитие технологий, которые могут как повысить безопасность, так и создать новые угрозы;
* человеческий фактор: уровень подготовки и осведомленности сотрудников о возможных угрозах и методах защиты;
* внешняя среда: общая криминогенная обстановка, включая активность киберпреступников и уровень организованной преступности в регионе;
* регуляторные изменения: новые законы и нормативные акты, которые могут повлиять на защиту данных и управление рисками;
* партнерские отношения: уровень безопасности и надежности третьих сторон, с которыми банк сотрудничает;
* финансовые стимулы: привлекательность банка как цели для преступников, основанная на его финансовом состоянии и репутации.

Численная классификация вероятностей реализаций различных потенциальных угроз представлена в таблице 3.2.

Таблица 3.2 – Вероятностно-временная шкала реализации угроз

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид угрозы отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

После описания численных оценок степени ущерба коммерческого банка вероятности реализации потенциальных угроз, возможно на основании этих данных оценить риски для каждой вышеописанной потенциальной угрозы. Оценка рисков будет представлена в следующем подразделе.

# 3.3 Оценка рисков

На основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем. В качестве максимального допустимого уровня риска положим 1, а максимальный интегральный (суммарный) уровень риска примем равным 4.

Далее в каждой строке таблицы проверяется, превышает ли данная угроза предельно допустимый уровень риска или нет. Если такое превышение имеет место, данная угроза должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

Оценка рисков представлена в таблице 3.3.

Таблица 3.3 – Оценка рисков банка

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Описание угрозы | Ущерб | Вероятность | Риск (Ущерб × Вероятность) | Методы защиты |
| Мошенничество с кредитными картами | 1 | 0,2 | 0,2 | Двухфакторная аутентификация,  cистемы мониторинга транзакций |
| Взлом системы и кража денежных средств | 3 | 0,3 | 0,9 | Многоуровневая аутентификация, шифрование данных |
| Утечка конфиденциальной информации | 2 | 0,4 | 0,8 | Политики доступа, шифрование конфиденциальных данных |
| Значительная кибератака с остановкой операций | 4 | 0,1 | 0,4 | Резервное копирование данных |
| Проблемы с доступом к системам из-за вирусов | 2 | 0,5 | 1 | Антивирусное ПО |
| Полное прекращение операций из-за атаки | 5 | 0,1 | 0,5 | Мониторинг состояния систем |
| Фишинг, приводящий к потере данных клиентов | 2 | 0,4 | 0,8 | Фильтрация электронной почты |
| Атака на систему защиты (DDoS) | 4 | 0,4 | 1,6 | Мониторинг сетевого трафика |
| Атака с использованием вредоносного ПО | 4 | 0,2 | 0,8 | Антивирусные и антишпионские программы |
| **Итого** |  |  | **7** |  |

Исходя из данных таблицы оценки рисков, риски каждой угрозы не превышают предельных допустимых значений (1), однако суммарный риск от всех угроз превышает максимальное допустимое значение – 5.

Следовательно, в системе безопасности набирается множество небольших угроз, которые необходимо решать комплексно. В этом случае выбираются угрозы с наибольшим уровнем риска (0,8), и работа по снижению вероятности или устранению этих угроз является наиболее приоритетной в разработке политики информационной безопасности.

# 4 Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов

В данном разделе будут рассмотрены средства и методы, которые необходимо применить для снижения вероятностей рисков или их устранения, а именно:

* стандарты менеджмента качества (правила и принципы работы с информацией для её защиты и безопасности);
* стандарты менеджмента качества: правила и принципы работы с информацией, направленные на её защиту и безопасность;
* процедуры: конкретные меры по охране информации, включая защиту персональных и конфиденциальных данных, а также правила доступа к носителям информации;
* **инструкции:** пошаговые алгоритмы действий для организации информационной защиты и соблюдения разработанных стандартов и процедур;
* план мероприятий по обучению персонала: программа обучения сотрудников политике информационной безопасности;
* аварийные планы: алгоритмы действий для восстановления работы организации в экстренных ситуациях.

Эти меры в совокупности помогут создать надежную систему защиты информации, минимизирующую риски и обеспечивающую безопасность как персональных, так и корпоративных данных. Постоянное обновление и адаптация этих методов к новым угрозам также являются ключевыми аспектами для поддержания высокого уровня информационной безопасности.

# Реализация средств защиты

Теперь давайте подробнее рассмотрим, какие средства защиты планируются и используются для каждого типа потенциальных угроз информационной безопасности.

# Несанкционированный доступ сотрудников

Одной из наиболее серьезных угроз для коммерческого банка является несанкционированный доступ к персональным и корпоративным данным сотрудниками. Такие атаки обычно направлены на копирование клиентских баз данных с персональной информацией для последующей передачи третьим лицам и конкурентам.

Авторизация является ключевым методом защиты от данного типа угроз. Она подразумевает предоставление сотрудникам прав на выполнение определённых действий, включая доступ к клиентским базам данных, а также процесс проверки этих прав при попытке их реализации.

В качестве реализации авторизации могут быть применены:

* для технических средств хранения информации: использование уникальных паролей для отдельных сотрудников или групп, а также внедрение двухфакторной аутентификации;
* для физических средств хранения информации: выдача личных ключ-карт и организация охраны, а также пропускного режима в помещениях, где находятся персональные и конфиденциальные данные

# Санкционированный доступ сотрудников

Авторизация защищает информацию от несанкционированного доступа сотрудников. Однако, что делать, если сотрудник с правами доступа намерен совершить неправомерные действия?

Одним из ключевых методов минимизации рисков внутренних угроз является реализация принципа наименьших привилегий. Каждому сотруднику следует предоставлять только те права доступа, которые необходимы для выполнения его задач. Это значительно ограничивает возможности неправомерных действий, даже если у сотрудника есть доступ к критически важной информации.

Вторым важным шагом является четкое определение ролей и обязанностей. Это помогает избежать ситуаций, когда один сотрудник имеет слишком много полномочий. Необходимо разделять ответственность: одни сотрудники могут вводить данные, а другие — проверять их или удалять.

Регулярный мониторинг действий сотрудников, имеющих доступ к чувствительной информации, а также ведение журналов аудита, позволяют выявлять подозрительную активность. Наличие системы, фиксирующей все действия с данными, дает возможность быстро реагировать на любые аномалии.

Технологические решения, такие как системы обнаружения вторжений (IDS) и системы предотвращения утечек данных (DLP), служат для выявления и предотвращения неправомерных действий. Эти системы могут автоматически оповещать о подозрительной активности.

Таким образом, защита информации от неправомерных действий со стороны сотрудников требует комплексного подхода, включающего как организационные, так и технические меры. Создание культуры безопасности, поддерживаемой четкими процессами и современными технологиями, поможет существенно снизить риски, связанные с внутренними угрозами. Важно помнить, что безопасность информации — это не разовая задача, а постоянный процесс, который требует адаптации к изменениям в организации и возникающим угрозам.

# Несанкционированный доступ хакеров и их группировок

Несанкционированный доступ к хранилищам данных почти всегда осуществляется третьими лицами, а не сотрудниками банка. Наиболее распространенной угрозой безопасности является несанкционированный доступ хакеров или групп хакеров к базам данных клиентов с целью получения персональных данных о клиентах банка, таких как номера телефонов, номера автомобилей, паспорта, кредитная информация, полные имена и другие личные данные.

Самым простым решением для снижения потенциала угроз является установка антивирусного и лицензионного программного обеспечения на рабочее оборудование и компьютеры. Однако этих мер недостаточно для обеспечения необходимого уровня защиты информационных ресурсов.

Также должны проводиться мероприятия по обеспечению безопасности в компьютерных сетях в коммерческого банка:

* организация безопасности в локальной сети;
* для технических средств хранения информации: использование уникальных паролей для отдельных сотрудников или групп, а также внедрение двухфакторной аутентификации;
* обеспечение невозможности несанкционированного доступа к локальной сети из внешней сети;
* обеспечение защищённости каналов связи и каналов передачи данных;
* использование современных криптографических методов шифрования для информационных процессов передачи данных;
* использование экранирования;
* ведение аудита и протоколирование всех выполняемых действий;
* организация обучения сотрудников стандартам и методам безопасного взаимодействия с информацией.

# Проникновение третьих лиц на рабочие места

В связи с тем, что в коммерческом банке значительное количество информационных средств хранится на физических носителях (жесткие и магнитные диски, бумажные документы), существует риск утечки или несанкционированного доступа к этой информации.

Для минимизации рисков, связанных с этой угрозой, следует применять разнообразные технические средства защиты. К ним относятся:

* организация обучения сотрудников стандартам и методам безопасного взаимодействия с информацией.
* введение строгого пропускного режима для сотрудников и посетителей;
* установка надежных дверных замков и систем контроля доступа, таких как магнитные или электронные ключ-карты;
* использование сейфов для хранения критически важных данных и документов;
* организация охраны помещений для предотвращения несанкционированного доступа;
* установка камер видеонаблюдения для мониторинга и записи событий в критически важных зонах.

Дополнительно важно проводить регулярные проверки и аудит систем безопасности, а также обучать сотрудников основам информационной безопасности, чтобы предотвратить возможные инциденты и повысить общий уровень защиты данных.

# Человеческий фактор

Человеческий фактор представляет собой совокупность характеристик, влияющих на надежность и эффективность сотрудников банка в различных ситуациях. На него оказывают влияние множество факторов, включая возраст, эмоциональное состояние, физическое здоровье, предрасположенность к распространенным ошибкам и когнитивным искажениям.

Человеческий фактор является основной причиной большинства непреднамеренных ошибок, совершенных сотрудниками банка. Эти ошибки могут возникать из-за чрезмерной самоуверенности, недостаточного обучения, непонимания сути процессов или недостатка знаний. Важно отметить, что полностью исключить возможность возникновения непреднамеренных ошибок, связанных с человеческим фактором, невозможно.

При разработке политики информационной безопасности необходимо классифицировать средства, меры и методы, направленные на снижение вероятности таких угроз. Эти меры также должны минимизировать потенциальный ущерб для банка в случае реализации угроз.

Методы и средства снижения вероятности непреднамеренных угроз, связанных с человеческим фактором, могут включать:

* установка камер видеонаблюдения для мониторинга и записи событий в критически важных зонах.
* установление четких правил и стандартов работы, обязательных для всех сотрудников банка. Это поможет создать единую культуру безопасности;
* регулярное обучение и повышение квалификации сотрудников, включая обсуждение нововведений и изменений на рабочих совещаниях. Таким образом, можно снизить риски, связанные с недостаточной квалификацией и устаревшими знаниями;
* распределение задач между сотрудниками для обеспечения внимания к деталям и уменьшения вероятности ошибок, возникающих из-за перегрузки;
* снижение влияния микро-менеджмента, который может негативно сказаться на моральном состоянии сотрудников. Это можно достичь четким распределением задач и использованием систем управления проектами;
* создание культуры открытости и доверия, где сотрудники могут сообщать о своих ошибках без страха наказания. Это поможет выявить проблемы на ранней стадии и предотвратить их повторение;
* внедрение систем автоматизации для рутинных задач, что снизит вероятность человеческой ошибки и освободит время для более сложных задач;
* проведение анонимных опросов для выявления проблемных областей и действий, которые могут вызвать недовольство или затруднения у сотрудников. Это поможет улучшить атмосферу в коллективе и выявить скрытые риски;
* использование системы вознаграждений для сотрудников, которые демонстрируют высокий уровень ответственности в вопросах безопасности. Это может стимулировать их более внимательное отношение к соблюдению стандартов.
* регулярное проведение симуляций и тренингов по реагированию на инциденты безопасности. Это поможет сотрудникам лучше подготовиться к реальным ситуациям и отработать правильные действия.

Эти меры должны быть задокументированы в политике информационной безопасности банка и регулярно пересматриваться, чтобы адаптироваться к изменяющимся условиям и новым угрозам. Комплексный подход к управлению человеческим фактором существенно повысит уровень информационной безопасности и защитит активы банка.

# Программа обеспечения информационной безопасности

Обеспечение информационной безопасности в коммерческом банке является ключевым аспектом управления организацией, необходимым для достижения её стратегических целей и задач. Хранящиеся в банке персональные данные клиентов и финансовая информация требуют повышенного внимания к вопросам безопасности.

Для успешного внедрения информационной безопасности в банке недостаточно лишь разработки документации по политике безопасности и реализации технических средств защиты. Необходима систематическая и планомерная деятельность, охватывающая все уровни организации. Это включает в себя создание инструкций с детальными алгоритмами действий по обеспечению информационной защиты, а также разработку стандартов и процедур. Также важно организовать мероприятия по обучению персонала и тестированию знаний сотрудников, имеющих доступ к критически важным информационным ресурсам.

Можно выделить следующий план мероприятий:

* использование системы вознаграждений для сотрудников, которые демонстрируют высокий уровень ответственности в вопросах безопасности. Это может стимулировать их более внимательное отношение к соблюдению стандартов.
* разработка требований к информационной безопасности и документирование обязанностей для всех сотрудников банка;
* предоставление четких инструкций по информационной безопасности для сотрудников всех уровней;
* теоретическое и практическое обучение сотрудников основным принципам информационной безопасности с последующей проверкой их знаний;
* организация восстановительных работ в случае реализации угроз безопасности;
* плановое резервное копирование данных и информации на жестких дисках;
* регулярное обновление баз данных вирусов в антивирусных системах;
* обеспечение физической безопасности средств хранения данных (на электронных и бумажных носителях) с использованием сейфов, помещений с видеонаблюдением и системой пропускного режима;
* документирование порядка действий в случае различных нарушений информационной безопасности.

Все эти мероприятия должны быть зафиксированы в политике информационной безопасности банка и внедрены в практику. Важно также периодически пересматривать и обновлять эти меры в зависимости от изменяющихся условий и новых угроз. Таким образом, комплексный подход к обеспечению информационной безопасности позволит банку эффективно защищать свои активы и поддерживать доверие клиентов.

# Заключение

Политика информационной безопасности коммерческого банка разработана таким образом, чтобы полностью отражать концепции, стандарты, директивы, процедуры и планы действий, соответствует всем общим принципам построения политики информационной безопасности и гарантирует доступность, целостность и конфиденциальность информационных средств.

Политика также реализует все цели и задачи, поставленные ранее. Кроме того, она должна быть реализована на всех уровнях коммерческих банков в соответствии с инструкциями, процедурами и планами действий, изложенными выше.

Описанные меры и методы считаются эффективными для снижения риска всех перечисленных угроз информационной безопасности до уровня ниже предельно допустимого.

Обеспечение реализации политики на всех уровнях коммерческого банка должно проверяться раз в год, а политика информационной безопасности должна пересматриваться и корректироваться каждые пять лет.