МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Факультет информационных технологий  
Кафедра: Информационные системы и технологии  
Специальность: Информационные системы  
Специализация: Инженер-программист

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**К ЛАБОРАТОРНОЙ РАБОТЕ НА ТЕМУ:**

Политика информационной безопасности банка

Студент: Смирнов Евгений Михайлович

Руководитель работы: Савельева Маргарита Геннадьевна

Заведующий кафедрой: Блинова Евгений Александровна

Минск 2025

**Оглавление**

[1 Обоснование актуальности, цели и задачи разработки политики информационной безопасности в банке 3](#_Toc209422024)

[2 Объекты защиты. Описание структуры банка, периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности 5](#_Toc209422025)

[3 Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних 8](#_Toc209422026)

[4 Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты 10](#_Toc209422027)

[5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 11](#_Toc209422028)

[Выводы и предложения 15](#_Toc209422029)

# Обоснование актуальности, цели и задачи разработки политики информационной безопасности в банке

Деятельность банка, связанная с вовлечением активов банка в бизнес-процесс, всегда подвержена рискам, так как и активы, и бизнес-процессы могут подвергаться различного рода угрозам.

Информационная безопасность в банковских системах играет критически важную роль для защиты конфиденциальности, целостности и доступности финансовой информации.

Актуальность информационной безопасности в банковских системах подтверждается следующими аспектами:

1. Конфиденциальность данных: банковские системы содержат конфиденциальную информацию о клиентах, включая персональные данные, финансовые счета, транзакции и другие сведения. Защита этой информации от доступа несанкционированных лиц является критической задачей для обеспечения доверия клиентов и соответствия нормативным требованиям.

2. Целостность данных: банковские системы должны обеспечивать целостность данных, чтобы предотвратить искажение или модификацию информации несанкционированными лицами. Целостность данных необходима для сохранения точности финансовой информации и идентификации несанкционированных изменений.

3. Непрерывность бизнес-процессов: банковская деятельность зависит от непрерывности и доступности систем. Нарушения информационной безопасности, такие как кибератаки или вирусные атаки, могут привести к простоям или временной недоступности банковских услуг, что приводит к финансовым потерям и утрате клиентского доверия.

4. Соответствие нормативным требованиям: банковские институты обязаны соблюдать строгие нормы безопасности и конфиденциальности, установленные компетентными органами и законодательством. Нарушение нормативных требований может привести к финансовым штрафам, утрате лицензии или судебным преследованиям.

5. Защита от киберугроз: банковские системы являются привлекательной целью для киберпреступников, которые стремятся получить доступ к финансовым ресурсам и скрыть свою активность. Защита от мошенничества, вредоносных программ и других киберугроз является необходимой для минимизации рисков финансовых потерь и сохранения репутации банка.

6. Защита от внутренних угроз: банковские системы также нуждаются в защите от внутренних угроз, таких как несанкционированный доступ к данным со стороны сотрудников, конфликты интересов и злоупотребление привилегиями доступа. Эффективные механизмы аутентификации, авторизации и мониторинга должны быть введены, чтобы уменьшить подобные угрозы.

Наличие четкой и эффективной политики информационной безопасности является критически важным элементом для успешной и безопасной работы любого банка. Политика информационной безопасности в банке является основным документом, определяющим правила и процедуры защиты информации, и служит фундаментом для эффективной работы системы информационной безопасности банка.

Политика информационной безопасности банка — это официальный документ, который определяет набор правил, процедур и руководящих принципов, регулирующих управление, защиту и распределение информационных активов банка для обеспечения их конфиденциальности, целостности и доступности от различных угроз.  Она служит основополагающим документом для выработки более детальных правил и процедур и обеспечивает соответствие требованиям законодательства, снижает риски финансовых потерь и формирует имидж надежного партнера.

 Цели политики информационной безопасности банка:

* Обеспечение конфиденциальности, целостности и доступности информационных активов банка
* Защита финансовых активов и конфиденциальных данных клиентов от несанкционированного доступа
* Соблюдение требований законодательства и нормативных актов в области информационной безопасности
* Поддержание доверия клиентов и репутации банка как надежного финансового института
* Обеспечение непрерывности банковских операций и бизнес-процессов
* Минимизация финансовых и репутационных рисков, связанных с информационной безопасностью

Задачи политики информационной безопасности банка:

* Разработка и внедрение системы защиты от несанкционированного доступа к информационным ресурсам банка
* Создание организационной структуры управления информационной безопасностью с четким распределением ролей и ответственности
* Установление единых правил и процедур работы с конфиденциальной информацией для всех сотрудников банка
* Внедрение технических средств защиты информации (антивирусные программы, межсетевые экраны, системы обнаружения вторжений)
* Организация обучения персонала по вопросам информационной безопасности и повышения цифровой грамотности
* Разработка процедур реагирования на инциденты информационной безопасности и восстановления после них
* Создание системы мониторинга и контроля соблюдения требований информационной безопасности
* Обеспечение соответствия деятельности банка требованиям национального законодательства и международных стандартов

# Объекты защиты. Описание структуры банка, периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности

Объекты защиты банка включают его финансовые активы, клиентские данные, информационные системы, а также физическую инфраструктуру и репутацию. Структура банка состоит из внешних объектов (филиалы, центры банковских услуг, представительства) и внутренних (управления, отделы, операционные кассы). Периметр защиты включает внешние границы банка и все его активы. Внутренняя структура включает информационные системы, автоматизированные рабочие места и данные, защищаемые с помощью многоуровневой системы информационной безопасности, состоящей из операционного управления, службы управления рисками и внутреннего аудита.

Объекты защиты банка:

* 1. Финансовые активы (деньги, ценные бумаги, кредитные средства, принадлежащие банку и его клиентам);
  2. Информационные ресурсы (конфиденциальные данные клиентов, информация о транзакциях, банковские системы и программное обеспечение);
  3. Информационная инфраструктура (серверы, сетевое оборудование, каналы связи и автоматизированные рабочие места, используемые банком);
  4. Физическая инфраструктура (здания, помещения, банкомат, инфокиоски и другое оборудование, обеспечивающее безопасность и функционирование банка);

Субъекты информационных отношений в банке:

* + - 1. Клиенты банка (Физические лица, Юридические лица, Индивидуальные предприниматели, Государственные учреждения и организации);

1. Сотрудники банка (Руководящий состав, Менеджеры и специалисты по работе с клиентами, Операционисты и кассиры, IT-специалисты и администраторы систем, Сотрудники службы безопасности, Аудиторы и контролеры, Сотрудники службы внутреннего контроля);
2. Контрагенты и партнеры (Другие банки и финансовые организации, Платежные системы, Центральный банк и регулятор, Страховые компани, Брокерские и инвестиционные компании, Поставщики IT-услуг и программного обеспечения);
3. Государственные органы ( Центральный банк, Федеральная служба по финансовому мониторингу, Федеральная налоговая служба, Прокуратура и правоохранительные органы, Суды различных инстанций);
4. Третьи лица (Нотариусы и адвокаты, Оценочные компании, Аудиторские фирмы, Консалтинговые компании, СМИ и журналисты, Исследовательские организации);
5. Технические субъекты (Автоматизированные системы банка, Внешние информационные системы, Платежные шлюзы, Системы межбанковских расчетов, Кредитные бюро).



Рисунок 2.1 — Структура банка

Периметр защиты — это границы, внутри которых осуществляется защита объектов. Он включает:

1. Внешний периметр — обеспечение безопасности физических объектов, входных зон, а также коммуникационных каналов и сетей с целью предотвращения несанкционированного доступа.
2. Внутренний периметр — защита от внутренних угроз, включая действия сотрудников, а также обеспечение безопасности отдельных информационных систем и данных.

Внутренняя структура информационно-вычислительных систем (ИВС) банка включает в себя:

1. Аппаратное обеспечение: физические компоненты, такие как серверы, сетевое оборудование, системы хранения данных, компьютерное оборудование для сотрудников и банкоматы.
2. Программное обеспечение:

- операционные системы: платформа для работы всего аппаратного обеспечения.

- системы управлениябазами данных (СУБД): программы для создания, управления и работы с базами данных.

- банковские прикладные системы: специализированное ПО для выполнения банковских операций (управление счетами, кредитами, депозитами, платежами и т.д.).

- средства коммуникации: программное обеспечение для обмена информацией внутри банка и с внешними системами.

1. Базы данных (БД): централизованное хранилище всех данных, с которыми работает банк, включая информацию о клиентах, счетах, транзакциях и другую финансовую информацию.
2. Автоматизированные рабочие места (АРМ): компьютеризированные рабочие места сотрудников банка, оснащенные необходимым программным обеспечением для выполнения своих функций.
3. Коммуникационная инфраструктура: сеть, обеспечивающая связь между различными компонентами ИВС и между банком и клиентами (интернет, локальные сети, VPN).
4. Каналы взаимодействия с клиентами: системы для обслуживания клиентов, такие как интернет-банкинг, мобильные приложения, банкоматы, что позволяет им управлять своими финансами.

# Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних

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

Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и её 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 угрозы, вызванные ошибками в проектировании информационной системы и её элементов, ошибками в действиях персонала и т.п.
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к инфраструктуре Банка могут быть как внешними, так и внутренними.

Внешние источники угроз информационной безопасности включают:

* киберпреступные группировки и хакеры (организующие целенаправленные атаки на ИТ-инфраструктуру);
* злоумышленники, использующие ботнеты для проведения DDoS-атак;
* разработчики и распространители вредоносного ПО (вирусы, трояны, программы-вымогатели);
* мошенники, применяющие социальную инженерию и фишинг;
* недобросовестные или скомпрометированные поставщики и подрядчики (атаки на цепочки поставок).

Внутренние угрозы исходят от сотрудников, к ним относятся:

* сотрудники банка (злонамеренные действия или халатность — инсайдерские угрозы);
* персонал, совершающий мошеннические операции (злоупотребление полномочиями, хищение средств);
* сотрудники, допускающие ошибки или нарушения регламентов, приводящие к утечке данных или снижению уровня защиты;
* лица с несанкционированным доступом к системам и данным (например, бывшие работники или сотрудники без необходимых прав).

Преднамеренные угрозы:

* + - 1. Кибератаки и хакерская деятельность
      2. Вредоносное программное обеспечение
      3. Социальная инженерия и мошенничество
      4. Инсайдерские угрозы
      5. Атаки на цепочки поставок

Непреднамеренные угрозы:

Ошибки персонала

Технические сбои и ошибки

Недостатки в проектировании систем

Нарушения регламентов и процедур

* + - 1. Недостаточная подготовка персонала

1. Устаревшие технологии и процессы

Эти угрозы требуют комплексного подхода к обеспечению информационной безопасности, включающего технические, организационные и кадровые меры защиты.

# Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты

Оценка угроз, рисков и уязвимостей информационной безопасности банка подразумевает выявление слабых мест в системах (уязвимостей), потенциальных опасностей (угроз) и вероятных последствий для банка (рисков) с последующим внедрением мер для их устранения или минимизации.  К основным уязвимостям относятся ошибки в конфигурировании, слабое программное обеспечение, а к угрозам — кибератаки, социальная инженерия и утечки данных. Риски включают потерю или искажение данных, несанкционированный доступ и неправомерные транзакции.

Таблица 4.1 – Оценка рисков для банка

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Кибератака на систему платежей | 5 | 0,3 | 1,5 |
| Мошенничество с банковскими картами | 4 | 0,4 | 1,6 |
| Взлом системы интернет-банкинга | 5 | 0,2 | 1,0 |
| Утечка персональных данных клиентов | 4 | 0,3 | 1,2 |
| Копирование базы данных клиентов | 4 | 0,2 | 0,8 |
| DDoS-атака на банковские сервисы | 3 | 0,4 | 1,2 |
| Саботаж сотрудника | 4 | 0,1 | 0,4 |
| **Итого:** | **–** | **–** | **7,7** |

Определение и оценка рисков: выявление угроз и уязвимостей для определения эффективности существующих мер и выработки новых.

Риски могут включать:

* утечку конфиденциальной информации;
* потерю или недоступность важных данных;
* искажение данных;
* компрометацию банка по заказу конкурентов;

Разработка и внедрение мер по устранению выявленных проблем: планирование и реализация мер по снижению рисков (обновление программного обеспечения, обучение персонала, внедрение более надежных систем защиты).

Постоянный мониторинг, регулярная оценка и обновление мер защиты в ответ на появление новых угроз и изменение технологического ландшафта.

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

Меры по обеспечению информационной безопасности банка включают:

1. Организационные меры:

* обучение и повышение цифровой грамотности персонала: сотрудники должны понимать риски, уметь распознавать фишинговые атаки и соблюдать правила информационной безопасности.
* разработка политик и процедур: создание правил, регламентирующих работу с конфиденциальной информацией и использование IT-систем.
* контроль доступа: внедрение системы разграничения прав доступа к информационным системам, чтобы сотрудники имели доступ только к той информации, которая необходима им для выполнения своих обязанностей.
* физическая безопасность: защита помещений с серверным оборудованием и конфиденциальными документами, организация пропускного режима.

1. технические меры (шифрование, межсетевые экраны, антивирусы, DLP-системы, резервное копирование):

* шифрование данных: защита информации путем её преобразования в нечитаемый вид, как при передаче, так и при хранении.
* межсетевые экраны (брандмауэры): барьер между внутренней банковской сетью и внешними сетями, контролирующий входящий и исходящий трафик.
* антивирусные программы и средства: защита от вредоносного ПО, которое может использоваться для кражи данных или нарушения работы системы.
* системы обнаружения и предотвращения вторжений (IDS/IPS): мониторинг сетевой активности для выявления подозрительной активности и автоматического блокирования атак.
* DLP-системы (Data Loss Prevention): программное обеспечение, предотвращающее утечки конфиденциальных данных из защищенного периметра организации.
* резервное копирование данных (бэкап): создание копий данных для последующего восстановления в случае их потери или повреждения.

1. криптографическая защита (шифрование данных);
2. многофакторная аутентификация: подтверждение личности пользователя с использованием нескольких способов (пароль, SMS-код, биометрия), что значительно повышает безопасность доступа к системам.
3. постоянный мониторинг системы для выявления и предотвращения кибератак и утечек данных.
4. защита каналов связи: контроль и шифрование данных, передаваемых по электронной почте, мессенджерам и облачным сервисам.

В целях минимизации рисков информационной безопасности в банках разрабатывается и утверждается политика информационной безопасности, в соответствии с которой создается, эксплуатируется и совершенствуется система обеспечения информационной безопасности.

Политика информационной безопасности разрабатывается на основе накопленного банком опыта в области обеспечения информационной безопасности, результатов идентификации активов, подлежащих защите, результатов оценки рисков информационной безопасности с учетом особенностей бизнеса и технологий, требований законодательства, в том числе нормативных правовых актов Национального банка, а также интересов и бизнес-целей конкретного банка.

Основные компоненты программы безопасности:

1. Защита физической инфраструктуры: обеспечение безопасности зданий, помещений и оборудования банка;

1. Защита информационных систем: включает безопасность данных, защиту от кибератак и обеспечение бесперебойной работы банковских систем;
2. Защита финансовых и материальных ресурсов: меры по предотвращению хищений, отмывания денег и других финансовых преступлений;
3. Безопасность клиентов: защита личных данных и средств клиентов, а также предотвращение мошеннических действий, направленных против них;
4. Безопасность сотрудников: обеспечение безопасных условий труда и защиты от внутренних угроз.
5. Управление рисками: анализ и оценка угроз, а также разработка планов по их минимизации и реагированию на инциденты.

Банк осуществляет постоянный контроль за соблюдением законодательства и внутренних регламентов в области информационной безопасности. Для этого формируется система отчетности, позволяющая оценивать текущие риски и поддерживать устойчивость работы ИТ-инфраструктуры.

Соблюдение установленных требований к системе информационной безопасности является необходимым условием для поддержания должного уровня защиты информации и обеспечения надежности предоставляемых услуг.

Требования к системе информационной безопасности должны быть документально закреплены в соответствии со стандартом финансовых услуг и технологий СФУТ 9.02-2024 «Банковская деятельность. Обеспечение информационной безопасности. Требования к документации по обеспечению деятельности в области информационной безопасности», утвержденным постановлением Правления Национального банка Республики Беларусь.

Общие требования к системе информационной безопасности банка:

1. Назначение и распределение ролей и обеспечение доверия к работникам банка: банком определяются и документально закрепляются роли его работников. Формирование и назначение ролей работникам банка осуществляются с соблюдением принципа предоставления минимальных прав и полномочий, необходимых для выполнения ими своих служебных (должностных) обязанностей. Ответственность определяется в должностных (рабочих) инструкциях, положениях о структурных подразделениях, организационно-распорядительных или иных документах банка. С целью предупреждения возникновения и снижения рисков информационной безопасности не допускается совмещение в рамках одной роли функций разработки и сопровождения программного обеспечения автоматизированной банковской системы его разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора информационной безопасности, выполнения операций в автоматизированной банковской системе и контроля их выполнения. Обязанности работников банка по выполнению требований по информационной безопасности включаются в трудовые договоры (контракты) и (или) должностные (рабочие) инструкции. Работники банка привлекаются к ответственности за невыполнение требований по информационной безопасности в соответствии с законодательством.
2. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированной банковской системы: в разрезе обеспечения информационной безопасности рассматриваются следующие общие стадии жизненного цикла автоматизированной банковской системы:

**-** разработка технических заданий;

**-** проектирование;

**-** создание и тестирование;

**-**приемка, включая оценку соответствия (испытания, аттестация системы защиты информации информационной системы и т.д.), и ввод в эксплуатацию;

**-** эксплуатация;

**-** сопровождение и модернизация;

**-** вывод из эксплуатации.

1. Защита от несанкционированного доступа к информации, объектам, информационным ресурсам, управление таким доступом и регистрацией всех действий в автоматизированной банковской системе и т.д.: банком применяются меры, направленные на обеспечение защиты от несанкционированного доступа, повреждения или нарушения целостности данных о действиях и операциях, а также меры по защите информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и работников банка. Все попытки несанкционированного доступа к такой информации регистрируются. Доступ к данным о действиях и операциях предоставляется только с целью выполнения служебных (должностных) обязанностей.
2. Антивирусная защита: целью обеспечения информационной безопасности средствами антивирусной защиты является защита хранимой и обрабатываемой в банке информации от раскрытия, уничтожения, блокирования, модификации, копирования, а также защита используемых программных средств. Задачами антивирусной защиты являются: определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления; проведение профилактических работ с применением антивирусных диагностических средств; непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации информационной и (или) автоматизированной систем.
3. Использование ресурсов глобальной компьютерной сети Интернет (далее – сеть Интернет): доступ к сети Интернет предоставляется ограниченному кругу работников банка в целях выполнения ими служебных (должностных) обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и сервисам. Решение об использовании сети Интернет с указанием целей такого использования принимается руководством банка. Использование сети Интернет в неустановленных целях запрещается.
4. Использование средств криптографической защиты информации (далее – СКЗИ): криптографическая защита информации используется в целях защиты от возможных атак, а также соответствия требованиям, предъявляемым при взаимодействии с международными платежными системами. В банке используют аппаратные модули безопасности для управления ключами, программное обеспечение для шифрования данных и система для генерации электронной подписи.
5. Защита банковских платежных технологических и банковских информационных технологических процессов: банком документируется банковский платежный технологический процесс. Документально определяются перечни программного обеспечения, устанавливаемого и (или) используемого в компьютерах и автоматизированных банковских системах, необходимого для выполнения конкретных банковских платежных технологических процессов. Выполнение данных требований контролируется, результаты контроля документируются. Банковские информационные технологические процессы документируются. Если данный технологический процесс реализован вне автоматизированной банковской системы программно-технические средства, его реализующие, изолируются от автоматизированной банковской системы на сетевом уровне. Документально определяются перечни программного обеспечения, устанавливаемого и (или) используемого для выполнения банковских информационных технологических процессов.

# Выводы и предложения

В ходе выполнения работы было установлено, что информационная безопасность является критически важным компонентом деятельности банка, обеспечивающим защиту информационных и финансовых активов, доверие клиентов и соответствие законодательным и нормативным требованиям.

Анализ показал, что:

* Информационные активы банка нуждаются в комплексной защите на организационном, техническом и правовом уровнях;
* Источниками угроз могут быть как внешние субъекты (хакеры, кибер-преступные группировки, недобросовестные поставщики), так и внутренние (сотрудники банка, персонал подрядчиков);
* Основные риски связаны с кибератаками, утечкой персональных данных клиентов, мошенничеством, а также ошибками персонала;
* Для эффективной защиты необходима реализация комплексной политики информационной безопасности, охватывающей технические, организационные и административные меры.

Предложения по совершенствованию системы информационной безопасности банка:

* Усилить организационные меры — проводить регулярное обучение сотрудников по вопросам ИБ, повышать их цифровую грамотность и внедрять практику тестирования на устойчивость к социальным атакам (фишинг, социальная инженерия).
* Совершенствовать систему управления доступом, основываясь на принципах минимальных прав и многофакторной аутентификации.
* Развивать систему мониторинга и анализа событий информационной безопасности (SIEM) для своевременного выявления атак и аномальной активности.
* Внедрить и поддерживать в актуальном состоянии систему управления инцидентами информационной безопасности, включающую процедуры реагирования и восстановления.
* Повысить уровень криптографической защиты данных, включая использование современных средств СКЗИ и аппаратных модулей безопасности.
* Усилить контроль за использованием внешних поставщиков и подрядчиков через договорные обязательства, аудит и требования к соблюдению норм ИБ.

Таким образом, комплексный подход к организации информационной безопасности, включающий правовые, организационные, технические и кадровые меры, позволит банку минимизировать риски, обеспечить надежность своей деятельности и укрепить доверие клиентов.