МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ   
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информационных систем и технологий

Специальность 1-40 05 01 «Информационные системы и технологии»

**Отчёт**

по дисциплине «Основы информационной безопасности»

**Исполнитель**

студент 2 курса 3 группы Д.А.Кальчевский

**Руководитель**

Преподаватель Н.В.Ржеутская

**Содержание**

[**Введение 2**](#_Toc115623400)

[**Описание структуры банка 4**](#_Toc115623401)

[**Принципы организационной структуры банков 4**](#_Toc115623402)

[**Примерная структура коммерческого банка 5**](#_Toc115623403)

[**Структура коммерческого банка в виде схемы: 6**](#_Toc115623404)

[**Оценка рисков 7**](#_Toc115623405)

[**Разработка мер защиты 8**](#_Toc115623406)

[**Выводы 10**](#_Toc115623407)

# **Введение**

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. В нашем случае это крупное кредитное учреждение (Банк). С учетом этого рассмотрим следующее определение политики безопасности.

**Политика безопасности** – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;

- определение ролей субъектов информационных отношений.

Результатом разработки политики безопасности является комплексный документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Этот документ является методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:

Основные положения информационной безопасности организации;

- область применения политики безопасности;

­­­­- цели и задачи обеспечения информационной безопасности организации;

- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

Согласно международному стандарту ISO/IEC 27001, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика информационной безопасности предприятия как минимум включала:

– определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации

– изложение целей и принципов информационной безопасности, сформулированных руководством

– краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

– соответствие законодательным требованиям и договорным обязательствам;

–  требования в отношении обучения вопросам безопасности;

– предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

– управление непрерывностью бизнеса;

– ответственность за нарушения политики безопасности.

– определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности

–  ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

– Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

# **Описание структуры банка**

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

Структуру банка определяют внешние требования к нему и особенности его работы.

**К внешним условиям относятся:**

1)Указания владельцев банка;

2)Цели создания данной конкретной организации;

Ее место в финансово-экономической системе страны или региона.

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.

Единого подхода, шаблона для банковской структуры в рыночной экономике не встречается, но есть некоторые общие принципы и распространенные варианты.

## Принципы организационной структуры банков

Можно выделить несколько подходов к построению внутренней среды банка:

1)Исходя из направлений деятельности, основных функций;

2)Ориентируясь на главных внешних потребителей банковского продукта;

3)Сочетая в себе два первых варианта, сообразно конкретной ситуации.

4)Чисто функциональный подход представить трудно. В таком случае пришлось бы собрать в одном кредитном управлении специалистов по выдаче займов физическим лицам и организациям; в управлении расчетных операций также объединились бы и платежи предприятий, и переводы по пластиковым картам.

Ориентация на крупных потребителей банковских услуг оказывается ближе к реальности. В спектре банковских операций удобно объединить работу с частными лицами в подразделение розничных операций, обслуживание организаций – в департамент корпоративного бизнеса.

В этом случае банк получит, как минимум, два кредитных управления, два управления развития, и некоторые другие структуры сходные по сути работы, но имеющие своего клиента.

Аналогичным образом дублируются подразделения банка по региональному признаку. Но слишком частое деление неизбежно создает проблемы с руководством системой, потому реальная внутренняя структуризация банков происходит по общности основных процессов и эффективности управления.

## Примерная структура коммерческого банка

Упрощенно внутреннюю систему коммерческого банка можно представить так:

**1) Высшее руководство банком** – собрание учредителей, другая подобная структура.

Непосредственным управлением операциями этот орган не занимается, но назначает исполнительные органы и контролирует их деятельность.

2) Правление банка во главе с председателем.

Это уже элемент текущего, оперативного управления. В его подчинении находятся руководители всех прочих подразделений.

Здесь обычно выделяют:

1)**Управление розничного бизнеса**. Сюда войдут отделы, обслуживающие частных лиц: кредитование, валютно-обменные операции, прием вкладов, операции с банковскими картами и пр.

2)**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.

3)**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.

4)**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.

5)**Бухгалтерия.** Структура обязательная для любого хозяйствующего субъекта, и всегда имеющая единое руководство.

6)**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.

7)**Юридическое управление**. Существует во всех банках, имеет в своем названии указание на специализацию и единое руководство.

8)**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.

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

10)**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.

11)**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.

12)**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.

Так обычно выглядит внутренняя структура [коммерческих банков](https://myfin.by/wiki/term/kommercheskie-banki-belarusi). Но крупные банковские организации и объединения имеют значительно больше подразделений, что продиктовано существенным разнообразием их интересов и операций.

Особую категорию составляют структурные элементы национальных банков государств. Это естественное отражение того факта, что национальный банк одно из главных звеньев экономической системы страны, его усилия направлены на поддержание и развитие этой системы.

## Структура коммерческого банка в виде схемы:



# **Оценка рисков**

Под угрозой информационной безопасности подразумевается воздействие на него, приводящие к ущербу.

— физической и логической целостности (уничтожение или искажение информации);

— конфиденциальности (несанкционированное получение);

— доступности (работоспособности);

— права собственности;

По происхождению:

— случайные (отказы, сбои, ошибки, стихийные явления);

— преднамеренные (злоумышленные действия людей);

По источникам:

— люди (персонал, посторонние);

— технические устройства;

— модели, алгоритмы, программы;

— внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

**Информационные риски:**

Технические устройства для взлома:

— вирусное ПО;

— удалённое подключение;

— использование флеш-носителей.

— Персонал – непосредственное скачивание важных данных или несанкционированное внесение изменений;

— посторонние – удалённый взлом, нацеленный на получение важной информации.

# **Разработка мер защиты**

На практике используют несколько групп методов защиты, в том числе:

• препятствие на пути предполагаемого похитителя, которое создают физическими и программными средствами;

• управление, или оказание воздействия на элементы защищаемой системы;

• маскировка, или преобразование данных, обычно – криптографическими способами;

• регламентация, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;

• принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;

• побуждение, или создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические.

Организационные средства защиты информации

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

• разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;

• проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;

• разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;

• внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;

• составляют планы восстановления системы на случай выхода из строя по любым причинам.

Технические средства защиты информации

Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:

• резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;

• дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;

• создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;

• обеспечение возможности использовать резервные системы электропитания;

• обеспечение безопасности от пожара или повреждения оборудования водой;

• установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

**Технические средства защиты информации**

Существуют разные виды обеспечения безопасности технических средств и систем информационной защиты. Методы и средства выбираются исходя из оценки прогнозируемых рисков – вероятностей и степени опасности:

* аппаратных сбоев в работе средств обработки, хранения, передачи, шифрования информации;
* несанкционированного доступа со стороны персонала предприятия или «внешних» злоумышленников;
* искажения, хищения, целенаправленного изменения информации посредством технических средств (посредством электромагнитного излучения, физического подключения к линиям связи, визуального или акустического наблюдения) или программного обеспечения

# **Выводы**

Каждая фирма или предприятие в наше время требует определённую политику информационной безопасности.

Банк, как никакая другая компания обязана содержать данные о своей компании, а также данные о клиентах и прочих сферах в целости и сохранности.

Разработка политики информационной безопасности осуществляется по определённым критериям и основывается на базовых принципах компании. В основу разработки входит описание структуры предприятия, создание определённых правил работы компании, проведение анализа целостности и создание объекта автоматизации данных.