Белорусский государственный технологический университет

Факультет информационных технологий

Кафедра программной инженерии

Практическое задание 2

По дисциплине «Основы информационной безопасности»

На тему «Разработка политики информационной безопасности бизнес-компании»

Выполнила:

Студентка 2 курса 2 группы

Глухова Д.В.

Вариант 6

Преподаватель: ст. пр. Ржеутская Н. В.

2023, Минск

**Введение**

В современном мире информационная безопасность становится одним из самых актуальных и насущных вопросов, особенно в контексте финансовых учреждений, таких как банки. Финансовый сектор играет важнейшую роль в глобальной экономике, и его безопасное функционирование имеет критическое значение не только для финансовых институтов, но и для всего общества. В этом контексте разработка и активная реализация политики информационной безопасности в банке приобретают стратегическое и незаменимое значение.

Банки - это не только места, где хранятся деньги и совершаются финансовые операции, но и хранилища огромных объемов конфиденциальной информации. Клиентские данные, финансовые транзакции, бухгалтерская информация, интеллектуальная собственность и многое другое сосредотачивается внутри банковских систем. Вследствие этого, они становятся привлекательной целью для киберпреступников, шпионов, и конкурентов, стремящихся нанести ущерб не только банкам, но и всей финансовой системе.

Опасности, с которыми сталкиваются банки, становятся все более разнообразными и изощренными с каждым днем. Кибератаки, включая вирусы, взломы, фишинг и многие другие виды атак, угрожают конфиденциальности, целостности и доступности данных. Следовательно, банки должны быть вооружены соответствующими стратегиями и средствами, чтобы предотвратить, выявить и реагировать на подобные угрозы.

Следует также учесть, что нарушения информационной безопасности могут иметь далеко идущие последствия. Это не только потеря данных и финансовых потерь, но и утрата доверия клиентов и партнеров, юридические последствия, репутационный ущерб и даже угроза национальной безопасности. Все это подчеркивает, насколько важно для банков наладить и эффективно управлять политикой информационной безопасности.

Таким образом, целью данного документа является обоснование неотложной потребности в разработке и реализации политики информационной безопасности для банка. Мы рассмотрим ключевые причины, почему этот вопрос стоит на переднем плане, и выявим роль данной политики в обеспечении устойчивости, надежности и конфиденциальности банковских операций. Безопасность информации становится фундаментальным аспектом, который позволяет банкам продолжать свою миссию обеспечения финансовой стабильности и долгосрочного роста в мире, где киберугрозы становятся все более угрожающими и сложными.

**Описание структуры бизнес-компании**

Функции в вестибюле и зоне обслуживания:

1. Входная зона:
   * Регистрация клиентов при входе.
   * Выдача токенов для управления очередью.
2. Кассовая зона:
   * Прием и выдача денежных средств.
   * Обмен валюты.
   * Погашение кредитов и взносы.
3. Терминалы самообслуживания:
   * Оплата счетов и переводы через терминалы.
   * Внесение/выдача наличных через банкоматы.
   * Информационные запросы о банковских продуктах.
4. Кассиры и операторы обслуживания:
   * Консультирование клиентов по банковским продуктам и услугам.
   * Работа с банковскими картами и чеками.
   * Решение операционных вопросов клиентов.
5. Контроль идентификации:
   * Проверка документов клиентов.
   * Использование биометрических данных для подтверждения личности.

Изменения и модернизации в обеспечении информационной безопасности:

1. Система электронной очереди:
   * Внедрение приложения для электронной записи в очередь.
   * Уведомление клиентов о своей очереди через мобильные устройства.
2. Бесконтактные технологии:
   * Внедрение бесконтактных карт и мобильных платежей для ускорения транзакций.
   * Технологии nfc для взаимодействия с терминалами.
3. Современные терминалы самообслуживания:
   * Обновление программного обеспечения терминалов для более широкого спектра операций.
   * Интеграция терминалов с мобильными приложениями банка.
4. Системы информационной безопасности:
   * Внедрение систем мониторинга для выявления подозрительной активности.
   * Обучение сотрудников правилам безопасности и распознаванию мошенничества.
5. Улучшенное обучение сотрудников:
   * Обучение персонала современным технологиям и методам обслуживания клиентов.
   * Инструктаж по эффективному использованию новых систем.
6. Идентификация и аутентификация:
   * Внедрение двухфакторной аутентификации для повышения защиты доступа к системам банка.
   * Обновление системы контроля идентификации с использованием биометрии.
7. Шифрование транзакций:
   * Обеспечение шифрования данных при проведении финансовых транзакций через терминалы и кассы.

Функции в зале ожидания:

1. Предоставление комфорта:
   * Предоставление удобных сидений и приятной атмосферы для клиентов, ожидающих обслуживание.
   * Обеспечение чистоты и порядка в зоне ожидания.
2. Информационное обслуживание:
   * Размещение информационных баннеров или экранов с актуальной информацией о продуктах и услугах банка.
   * Предоставление информации о текущих акциях и нововведениях.
3. Коммуникационные услуги:
   * Предоставление бесплатного wi-fi для клиентов.
   * Установка зарядных устройств для мобильных устройств.

Возможные изменения и модернизации в обеспечении информационной безопасности:

1. Контроль доступа:
   * Внедрение системы контроля доступа к зоне ожидания, чтобы предотвратить несанкционированный доступ.
2. Видеонаблюдение:
   * Установка камер видеонаблюдения для мониторинга безопасности в зоне ожидания.
   * Системы аналитики видео для выявления подозрительного поведения.
3. Киоски безопасности:
   * Установка киосков с экранами для показа информации о правилах безопасности, контактной информации и процедурах эвакуации.
4. Повышение автоматизации:
   * Внедрение электронных систем управления зоной ожидания для эффективного мониторинга и быстрого реагирования на потенциальные угрозы.
5. Обучение сотрудников:
   * Обучение сотрудников правилам безопасности, обнаружению подозрительных ситуаций и взаимодействию с посетителями в критических ситуациях.
6. Экстренные средства безопасности:
   * Установка экстренных кнопок и средств для быстрого вызова служб безопасности в случае необходимости.
7. Шифрование wi-fi:
   * Защита сети wi-fi в зоне ожидания с использованием современных методов шифрования.
8. Автоматизированные уведомления:
   * Внедрение автоматизированных систем оповещения в случае нештатных ситуаций или изменений в режиме работы банка.

Функции в отделениях/офисах:

1. Отделение кредитования:
   * Прием и обработка заявок на кредиты от физических лиц.
   * Оценка кредитоспособности клиентов.
   * Выдача и управление кредитами.
2. Отделение по работе с корпоративными клиентами:
   * Обслуживание корпоративных клиентов.
   * Разработка финансовых предложений для предприятий и организаций.
   * Управление корпоративными счетами и финансовыми операциями.
3. Отделение инвестиций и финансового консультирования:
   * Консультирование клиентов по вопросам инвестиций и финансового планирования.
   * Предоставление информации о финансовых инструментах, портфелях и стратегиях.

Возможные изменения и модернизации в обеспечении информационной безопасности:

1. Контроль доступа к кредитной информации:
   * Внедрение строгих систем контроля доступа к кредитной информации, предотвращение несанкционированного доступа.
2. Шифрование корпоративных данных:
   * Применение современных методов шифрования для защиты конфиденциальных данных корпоративных клиентов.
3. Системы мониторинга финансовых транзакций:
   * Использование систем мониторинга для выявления подозрительных финансовых операций и предотвращения мошенничества.
4. Усиление аутентификации корпоративных клиентов:
   * Внедрение многофакторной аутентификации для повышения безопасности при взаимодействии с корпоративными клиентами.
5. Обучение сотрудников по безопасности:
   * Проведение регулярных тренингов для сотрудников по правилам информационной безопасности и обнаружению мошенничества.
6. Физическая безопасность:
   * Установка систем видеонаблюдения и контроля доступа в отделениях для защиты от несанкционированного доступа.
7. Шифрование электронных писем:
   * Защита электронной переписки и обмена документами с клиентами с использованием шифрования.
8. Обеспечение конфиденциальности инвестиционных данных:
   * Создание защищенных сред для хранения и передачи конфиденциальной информации об инвестициях.

Функции в самообслуживании:

1. Банкоматы:
   * Снятие и внесение наличных.
   * Проверка баланса счета.
   * Погашение кредитов и взносы.
   * Обмен валюты.
2. Терминалы для онлайн-банкинга:
   * Оплата счетов и переводы между счетами.
   * Просмотр истории транзакций.
   * Обновление личной информации клиента.
   * Получение выписок.

Возможные изменения и модернизации в обеспечении информационной безопасности:

1. Шифрование банкоматных транзакций:
   * Внедрение современных методов шифрования для защиты данных при проведении транзакций через банкоматы.
2. Защита от клонирования карт:
   * Установка антиклонировочных устройств на банкоматах для предотвращения кражи данных с банковских карт.
3. Мониторинг систем банкоматов:
   * Использование систем мониторинга для выявления подозрительной активности вокруг банкоматов.
4. Биометрическая аутентификация:
   * Внедрение технологий биометрической аутентификации для усиления защиты при снятии наличных.
5. Защита от вредоносных устройств:
   * Установка антивирусного и антишпионского программного обеспечения на банкоматы для предотвращения угроз от вредоносных программ.
6. Обновление программного обеспечения:
   * Регулярное обновление программного обеспечения банкоматов и терминалов для закрытия уязвимостей и улучшения безопасности.
7. Безопасность онлайн-банкинга:
   * Использование современных алгоритмов шифрования для защиты данных в процессе онлайн-банкинга.
8. Многофакторная аутентификация:
   * Внедрение многофакторной аутентификации для доступа к онлайн-банкингу через терминалы.
9. Обучение пользователей:
   * Проведение обучающих сессий для пользователей по правилам безопасности при использовании банкоматов и терминалов.

Функции в офисе управления:

1. Руководство филиала/офиса:
   * Разработка стратегии и целей филиала/офиса в соответствии с общей стратегией банка.
   * Принятие стратегических решений, направленных на развитие и достижение целей.
   * Управление операционными процессами и персоналом.
2. Отдел по внутренней связи и координации:
   * Обеспечение эффективного внутреннего общения внутри филиала/офиса.
   * Координация деятельности различных отделов и подразделений.
   * Управление информационными потоками внутри офиса.

Возможные изменения и модернизации в обеспечении информационной безопасности:

1. Управление доступом:
   * Внедрение системы управления доступом для контроля доступа сотрудников к конфиденциальной информации и ресурсам.
2. Шифрование критических данных:
   * Шифрование критических данных и документов, которые обрабатываются в офисе управления.
3. Безопасность электронной почты:
   * Обеспечение защиты электронной переписки руководства от вредоносных программ и фишинговых атак.
4. Мониторинг информационных систем:
   * Внедрение систем мониторинга для отслеживания активности в информационных системах офиса управления.
5. Защита от внутренних угроз:
   * Разработка стратегии защиты от внутренних угроз, включая утрату данных и несанкционированный доступ.
6. Аутентификация и авторизация:
   * Внедрение строгих методов аутентификации и авторизации для обеспечения безопасности при доступе к важным системам.
7. Обучение персонала по безопасности:
   * Проведение регулярных обучающих сессий по вопросам информационной безопасности для сотрудников офиса управления.
8. Системы резервного копирования:
   * Введение систем резервного копирования для предотвращения потери важных данных и обеспечения их восстановления в случае необходимости.
9. Физическая безопасность офиса:
   * Обеспечение физической безопасности офиса, включая контроль доступа и видеонаблюдение.
10. Аудит информационной безопасности:

* Проведение периодических аудитов информационной безопасности для выявления уязвимостей и рисков.

**Оценка рисков**

Оценка рисков в информационной безопасности представляет собой систематический процесс, направленный на выявление, анализ и оценку потенциальных угроз, а также определение возможных последствий и вероятности их реализации. Для более конкретного понимания процесса оценки рисков, давайте рассмотрим основные аспекты, учитываемые при оценке рисков.

1. Ценность ресурсов:
   * Количественный подход: измерение стоимости ресурсов в денежных единицах, например, стоимость информации, оборудования, программного обеспечения.
   * Качественный подход: оценка значимости ресурсов с использованием категорий, таких как "критически важный," "важный," "менее важный."
2. Оценка значимости угроз:
   * Количественный подход: ранжирование угроз по степени их воздействия на ресурсы с учетом потенциальных финансовых потерь.
   * Качественный подход: определение угроз с использованием категорий, таких как "высокий," "средний," "низкий" в зависимости от потенциальных последствий.
3. Эффективность средств защиты:
   * Оценка текущих средств защиты: анализ того, насколько эффективно текущее информационное безопасности предотвращает угрозы.
   * Планируемые меры по управлению рисками: оценка планируемых средств защиты и их ожидаемой эффективности.
4. Определение вероятности реализации угрозы:
   * Привлекательность ресурса: оценка того, насколько ценен ресурс для потенциального злоумышленника.
   * Возможность получения дохода: рассмотрение возможности использования ресурса для финансовой выгоды злоумышленником.
   * Технические возможности угрозы: оценка технических навыков и средств, которые могут быть использованы при угрозе.
5. Дополнительные факторы:
   * Вероятность реализации угрозы: оценка вероятности того, что угроза будет реализована, учитывая привлекательность ресурса и технические возможности угрозы.
   * Степень легкости использования уязвимости: анализ того, насколько легко злоумышленник может использовать уязвимость в системе.

Оценка рисков в информационной безопасности является динамическим процессом, который требует постоянного мониторинга и анализа, особенно в контексте постоянно меняющейся угрозовой среды и технологических изменений. Понимание этих факторов позволяет банку эффективно выбирать и реализовывать средства управления информационной безопасностью.

**Меры защиты**

1. Управление персоналом:
   * Регулярные обучающие сессии и тренинги по ИБ для персонала, фокусирование на актуальных угрозах и методах защиты.
   * Внедрение системы наград и поощрений для сотрудников, активно соблюдающих правила информационной безопасности.
2. Физическая защита:
   * Регулярно проводите инспекции физической безопасности, проверяя системы видеонаблюдения, контроля доступа и другие технические средства.
   * Обеспечьте обучение персонала по процедурам физической безопасности и регулярно проводите учения на случай чрезвычайных ситуаций.
3. Планирование восстановительных работ:
   * Проводите регулярные учения по восстановлению после аварий, оценивая эффективность планов и идентифицируя области для улучшения.
   * Создайте подробные сценарии для тренировок, включая симуляцию различных видов атак и аварий.
4. Поддержание работоспособности:
   * Разработайте и поддерживайте тщательный план обновления и обслуживания it-инфраструктуры, включая резервное копирование данных и обновление программного обеспечения.
   * Внедрите системы мониторинга для оперативного обнаружения сбоев и проблем в работе it-систем.
5. Реагирование на нарушения режима безопасности:
   * Разработайте четкий и структурированный план реагирования на инциденты безопасности, включая определенные шаги и ответственных за их выполнение.
   * Проводите регулярные тренировки по реагированию на инциденты, вовлекая все звенья персонала.
6. Программно-технические меры безопасности:
   * Регулярно обновляйте системы и программное обеспечение, следите за выходом новых патчей и обеспечивайте быструю их установку.
   * Внедрите многофакторную аутентификацию для критически важных систем и данных.
7. Идентификация и аутентификация пользователей:
   * Используйте современные методы идентификации, такие как биометрия, для повышения надежности аутентификации.
   * Регулярно обучайте сотрудников соблюдению безопасных практик идентификации.
8. Управление доступом:
   * Применяйте принцип наименьших привилегий, ограничивая доступ к системам и данным только необходимыми пользователями.
   * Разработайте систему регулярного аудита для проверки соответствия прав доступа сотрудников и их актуальных обязанностей.
9. Протоколирование и аудит:
   * Ведите систематический аудит действий пользователей и системы для обнаружения подозрительной активности.
   * Используйте автоматизированные средства аудита для более эффективного мониторинга и анализа данных.
10. Криптография:
    * Применяйте криптографию для защиты конфиденциальных данных в хранилищах и в процессе передачи.
    * Регулярно обновляйте используемые алгоритмы шифрования с учетом современных стандартов безопасности.
11. Экранирование:
    * Внедрите системы фильтрации сетевого трафика для предотвращения вредоносных атак и защиты от нежелательного контента.
    * Проводите анализ угроз сетевой безопасности и регулярно обновляйте фильтры в соответствии с новыми угрозами.
12. Обеспечение высокой доступности:
    * Используйте резервные системы и проактивные меры для минимизации времени простоя при сбоях.
    * Регулярно проверяйте работоспособность резервных систем и обновляйте их по необходимости.

**Вывод**

Эти рекомендации формируют комплексный подход к обеспечению информационной безопасности в банке, сочетая в себе процедурные и технические меры для эффективной защиты от угроз.

Выводы

В ходе разработки проекта политики информационной безопасности для нашей бизнес-компании были выделены ключевые аспекты, необходимые для эффективной защиты информации и обеспечения устойчивости наших операций.

Оценка рисков позволила выявить потенциальные угрозы и уязвимости в наших информационных системах. Это стало отправной точкой для разработки конкретных мер безопасности, направленных на минимизацию рисков и укрепление общей защиты.

Разработанные меры защиты охватывают все уровни компании, включая обучение персонала, внедрение технологических средств защиты, планирование восстановительных работ и системный мониторинг. Этот комплексный подход позволяет нам не только предотвращать инциденты, но и эффективно реагировать на них, обеспечивая бесперебойную работу компании.

Важным элементом политики информационной безопасности стал баланс между безопасностью и удобством для наших сотрудников и клиентов. Мы стремимся создать безопасное окружение, не забывая о комфорте использования наших услуг.

Осуществление постоянного мониторинга и обновление политики в соответствии с изменяющейся угрозой является важным аспектом нашего подхода. Безопасность — это процесс, требующий постоянного внимания и усовершенствования.

В целом, разработанный проект политики информационной безопасности станет фундаментом для надежной защиты наших информационных активов и поддержания доверия наших клиентов и партнеров.