Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Разработка и внедрение политики безопасности организации или учреждения»

Выполнила:

Студентка 3 курса 5 группы

Кубик Елизавета Валентиновна

Проверил:

Берников Владислав Олегович

Минск 2021

**Лабораторная работа №1**

**Тема «Разработка и внедрение политики безопасности банка»**

Цель: разработать политику информационной безопасности банка, а также план мероприятий по ее реализации.

## Теоретические сведения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вредоносный код – содержащаяся в любых файлах последовательность символов, результат исполнения которых позволяет отнести ее к компьютерным вирусам или вредоносным программам.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных (УБПДн) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Обоснование актуальности, цели и задачи разработки ПИБ в банке

С развитием информационного общества появилась потребность в защите его главного движущего фактора - информации. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности общества показывает, что существуют различные и весьма реальные угрозы потери информации, приводящие к негативным последствиям. А развитие информационных технологий и их активное внедрение создает качественно новые угрозы несанкционированного воздействия на информационные ресурсы и информационные системы. В этих условиях информационная безопасность банков становится важнейшим элементом безопасности банка в целом. Под информационной безопасностью принято понимать защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Целью деятельности по обеспечению информационной безопасности банка является повышение надежности защиты информации в процессе ее обработки, хранения и передачи; обеспечение устойчивого функционирования банка и защита информационных активов, принадлежащих банку, его акционерам, инвесторам и клиентам от случайных (ошибочных) и направленных противоправных посягательств, разглашения, утраты, утечки, искажения, модификации и уничтожения охраняемых сведений; снижение угроз информационной безопасности до приемлемого для банка уровня.

Для достижения основной цели защиты информации система обеспечения информационной безопасности банка должна обеспечивать эффективное решение следующих задач:

* своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы банка;
* создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
* создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
* защиту от вмешательства в процесс функционирования информационной системы банка посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам банка (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
* обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* защиту от несанкционированной модификации используемых в корпоративной информационной системе банка программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
* защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
* обеспечение живучести криптографических средств защиты информации.

## Объекты защиты

Основными объектами системы информационной безопасности в банке являются:

* информационные ресурсы с ограниченным доступом, составляющие коммерческую, банковскую тайну или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы банка, независимо от формы и вида ее представления;
* процессы обработки информации в информационной системе банка информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной банковской среды.

В банке циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая, банковская информация, персональные данные), и открытые сведения.

Защите подлежит вся информация и информационные ресурсы банка, независимо от ее представления и местонахождения в информационной среде банка.

## Основные угрозы и их источники

В качестве возможных угроз нарушения информационной безопасности в банке рассматриваются три основных класса угроз:

* угрозы нарушения конфиденциальности информации;
* угрозы нарушения целостности информации;
* угрозы нарушения доступности информации.

Каждая угроза информационной безопасности расписывается и анализируется следующим образом: «источник угрозы информационной безопасности» - «способ несанкционированного доступа к активу» - «несанкционированные действия с активом» - «уровень реализации угрозы информационной безопасности» - «нарушение характеристики безопасности актива».

Для успешного осуществления мер по обеспечению ИБ банка необходимо иметь представление о возможных угрозах для него. Модели угроз и нарушителей (прогноз ИБ) являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ банка. Деятельность банка поддерживается входящей в его состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

* физического (линии связи, аппаратные средства и пр.);
* сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
* сетевых приложений и сервисов;
* операционных систем (ОС);
* систем управления базами данных (СУБД);
* банковских технологических процессов и приложений;
* бизнес-процессов банка.

В качестве основных источников угроз ИБ банком рассматриваются внешние, внутренние и комбинированные нарушители.

Внешние нарушители информационной безопасности:

* клиенты банка;
* лица, случайно или намеренно, получившие доступ к информационным активам банка через внешние телекоммуникационные каналы связи;
* конкурирующие кредитные организации;
* программисты-разработчики программных компонент, не являющиеся сотрудниками банка;
* компании, обеспечивающие поставку и ремонт компьютерной техники;
* спецслужбы и представители силовых ведомств, имеющие возможность применять специальные средства и способы атак на информационные активы банка;

Внутренние нарушители информационной безопасности:

* сотрудники банка, имеющие легальный доступ к ресурсам автоматизированной банковской системы;
* сотрудники банка, осуществляющие доступ к информационным активам с использованием технологии удаленного доступа;
* сотрудники банка, имеющие полномочия системного администратора или администратора информационной безопасности;
* программисты-разработчики программных компонент, являющиеся сотрудниками банка.

Комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно (в сговоре).

В зависимости от цели, квалификации, технического оснащения и прав доступа к информационным системам банка нарушители информационной безопасности могут реализовывать атаки на уровне сетевого оборудования, операционных систем, систем управления базами данных, сетевых приложений и сервисов, банковских приложений и сервисов, используя следующие способы несанкционированного доступа:

* внедрение вредоносного программного обеспечения;
* кража носителей информационных активов;
* кража технических средств обработки информационных активов;
* несанкционированное повышение привилегий сотрудника банка в системе;
* несанкционированные действия сотрудников банка в системе;
* физическое подключение к каналу связи с целью перехвата информации;
* внесение недекларированных возможностей и/или программных закладок;
* внедрение ложных сетевых сервисов;
* подмена доверенного объекта;
* навязывание ложного сетевого маршрута;
* удаленный запуск приложений и т.д.

Все способы несанкционированного доступа к активам могут быть направлены на преднамеренное или случайное копирование, модификацию, удаление, передачу по каналам связи и/или передачу на материальных носителях, с целью нарушения конфиденциальности, целостности и/или доступности актива.

## Оценка угроз, рисков и уязвимостей

В рамках деятельности по обеспечению информационной безопасности условная численная шкала для оценки ущерба банку от НСД следующая:

|  |  |
| --- | --- |
| Величина ущерба | Ущерб |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб банку |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение банка на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время банк терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От банка уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, банк на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Банк прекращает существование |

Таблица 5.1 – Таблица шкалы ущерба

В рамках деятельности по обеспечению информационной безопасности вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам следующая:

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НДС) |
| 0 | Данный вид атаки 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 |

Таблица 5.2 – Таблица шкалы вероятности угрозы

В рамках деятельности по обеспечению информационной безопасности оценка рисков следующая:

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб x Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 4 | 0,1 | 0,4 |
| Вирусы | 5 | 0,3 | 1,5 |
| DDoS-атаки | 2 | 0,2 | 0,4 |
| Пиратское ПО | 0 | 0 | 0 |
| Итого | 12 | 1 | 2,7 |

Таблица 5.3 – Таблица оценки рисков

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

Все меры обеспечения безопасности информационной системы Банка подразделяются на:

* Законодательные (правовые) меры защиты: действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы банка.
* Морально-этические меры защиты: нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или банка в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.
* Технологические меры защиты: разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений, периодическое подведение общего баланса всех банковских счетов и т.п.
* Организационные (административные) меры защиты: меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

## Вывод

В ходе работы мы вывели список возможных опасностей, которые могут произойти с информацией банка. Оценка рисков проводилась двумя способами: качественным и количественным. Оценив риски можно вывести список возможных мер безопасности и средства защиты, которые могут предотвратить или уменьшить шанс данных угроз.

На сегодняшний день абсолютно любые учреждения, компании, предприятия и т.д. имеют политику безопасности. ПБ является неотъемлемой частью у каждой компании, каждого учреждения. Политика определяет способы развертывания системы безопасности. Сюда входит правильная настройка компьютерных систем и сетей в соответствии с требованиями физической безопасности.

Однако технические аспекты — это не единственное, что определяется политикой. Она ясно устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, например, для администраторов. Она определяет поведение пользователей при использовании компьютерных систем, размещенных в организации.

Также из вышесказанного в работе следует, что при разработке политики информационной безопасности учреждения, в том числе и банка, необходимо учитывать модель злоумышленника. Чем адекватнее будет модель, тем более полно будет организована защита конфиденциальных данных. Таким образом, построение модели злоумышленника является существенным звеном в организации политики безопасности информационной безопасности на предприятии.