Учреждение образования

«Белорусский Государственный Технологический Университет»

Кафедра программной инженерии

Разработка политики информационной

безопасности банка

Выполнил: студент 3 курса 4 группы ФИТ

Лэ Никита Зыонгович

Минск 2020

**Определения**

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 данны**х – 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).

**1. Общие положения**

* 1. Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн банка от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.
  2. Безопасность персональных данных достигается путем исключения 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.
  3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.
  4. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.
  5. Состав объектов защиты представлен в Перечне персональных данных обрабатываемых в банке.

**2. Цели и задачи информационной безопасности банка**

* 1. Основными целями обеспечения ИБ являются:
* соответствие требованиям законодательства, требованиям надзорных и регулирующих органов;
* повышение стабильности функционирования багка в целом;
* достижение адекватности мер по защите от реальных угроз информационной безопасности;
* предотвращение и/или снижение ущерба от инцидентов информационной безопасности;
* повышение доверия к банку со стороны клиентов, контрагентов, партнеров, инвесторов и общественности в целом, повышение рейтинга банка и его инвестиционной привлекательности;
* защита законных прав банка и его работников, в случаях неправомерного использования или злоупотребления информационной инфраструктурой и информационными активами;
* формирование взвешенного подхода к защите от угроз ИБ посредством применения экономически и технически обоснованных, а также необходимых и достаточных защитных мер информационной безопасности;
  1. Основными задачами обеспечения ИБ являются:
* своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;
* создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;
* эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
* создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

**3. Объекты обеспечения информационной безопасности**

* 1. Автоматизированная система обработки информации банка является распределенной структурой, объединяющей в единую ИС подсистемы центрального аппарата, региональных филиалов. Основными объектами обеспечения информационной безопасности в банке признаются следующие элементы:
     1. информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством к государственной тайне, коммерческой тайне банка, открытая информация, необходимая для обеспечения нормального функционирования банка (в дальнейшем - защищаемая информация);
     2. средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
     3. программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы банка, с помощью которых производится обработка защищаемой информации;
     4. помещения, предназначенные для ведения закрытых переговоров и совещаний;
     5. помещения, в которых расположены средства обработки защищаемой информации;
     6. технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.
  2. Подлежащая защите информация может находиться:
     1. на бумажных носителях;
     2. электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
     3. передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
     4. в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
     5. записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны и др.).

**4. Политика физической безопасности**

* 1. Помещения, которые должны быть оборудованы дополнительными устройствами регистрации, контроля и поддержания заданных характеристик (например, система автоматического пожаротушения, контроля влажности, принудительной вентиляции, кондиционирования воздуха, защиты от статического электричества и т.п.), в соответствии с НПА РБ или правилами эксплуатации оборудования, размещенного в таких помещениях, и требуемых для соблюдения гарантийных обязательств производителя, должны быть полностью укомплектованы подобными устройствами.
  2. В помещениях, в которых размещается имущество банка должна иметься возможность организации круглосуточной охраны. В помещениях, расположенных в зданиях, в которых возможно использование услуг служб централизованной охраны здания, охрана должна осуществляться силами таких служб. В помещениях, расположенных в зданиях без служб централизованной охраны, охрана должна осуществляться за счет привлечения специализированных организаций, предоставляющих услуги по круглосуточной охране. Допускается в рабочее время использование услуг служб охраны в режиме «вызов по необходимости», в нерабочее время помещения должны сдаваться под охрану с применением средств охранной сигнализации или с физическим наблюдением за помещениями.
  3. Периметр зданий, в которых располагаются помещения банка, должен охраняться посредством систем видеонаблюдения с возможностью хранения информации, а также вывода информации на пульт в помещении охраны.
  4. Все помещения банка должны быть оборудованы дверьми, закрываемыми на замок.
  5. Должен быть предусмотрен механизм установления личности, осуществляющей санкционированное вскрытие помещенийбанка, (например, проверка удостоверения личности, применение систем контроля и управления доступом, роспись за получения ключа от помещений на посту охраны и т.п.).
  6. Отдельные группы помещений, нахождение в которых посторонних лиц не требуется (например, архивные помещения), могут отделяться дополнительными дверьми, иными средствами ограничения доступа, опечатываться или физически располагаться удаленно (например, на других этажах или частях здания и т.п.).
  7. Доступ в помещения банка, и его филиалов, где хранятся и обрабатываются персональные данные, осуществляется в соответствии Перечнем должностей работников, который утверждается Руководителем банка.
  8. Работники не должны оставлять свои рабочие кабинеты без наблюдения. В случае, если помещение остается без наблюдения, помещение должно быть закрыто на замок.
  9. Работники не должны пытаться проникнуть в помещения, доступ к которым ограничен, не имея на это соответствующих прав.
  10. Нахождение посетителей или представителей сторонних организаций в помещениях банка должно контролироваться сопровождающими лицами из числа работников банка, допущенных в данные помещения или охранником.

**5. Правила эксплуатации электронных устройств**

* 1. Размещение экранов АРМ, обрабатывающих информацию ограниченного доступа, должно исключать возможность их просмотра лицами, не допущенными к данной информации.
  2. При использовании систем видеонаблюдения, такие системы должны быть установлены в местах, исключающих просмотр содержимого экранов АРМ, обрабатывающих информацию ограниченного доступа, а также исключающих просмотр вводимых паролей, кодов и т.п.
  3. Системные блоки АРМ, периферийное оборудование должно быть опечатано или оборудовано иным способом ограничения их несанкционированного вскрытия.
  4. Работникам банка запрещено подключать или устанавливать собственные компьютеры, периферийные устройства, в том числе съемные носители информации, комплектующие к АРМ и корпоративной сети банка без согласования с администратором безопасности или лицом его заменяющим.
  5. Все электронные устройства должны проходить профилактическое обслуживание. Такое обслуживание должно проводиться регулярно, но не реже сроков, указанных в технической документации на устройства или нормативных актах банка.

Профилактическое обслуживание должно производиться силами квалифицированных работников банка, если иное не определено производителем оборудования.

* 1. Все АРМ, предназначенные для выполнения работниками своих должностных обязанностей, должны быть оборудованы источниками бесперебойного питания.
  2. Сетевые, питающие и иные кабеля должны быть проложены с соблюдением стандартов и должно быть исключено повреждение таких кабелей при повседневной работе, а также минимизировать вероятность получения травмы работниками, вызванных нарушениями укладки таких кабелей.
  3. Перед передачей (в том числе для ремонта) сторонним организациям, списанием или прекращением использования оборудования, участвовавшего в обработке информации ограниченного доступа, должна быть проведена проверка, с целью исключения попадания такой информации третьим лицам.

1. **Политика обеспечения управления доступом**
   1. Работникам банка запрещено осуществление противоправных действий, включая деятельность по получению несанкционированного доступа к любой АС; нанесение ущерба и нарушение работы АС; перехват паролей или иной способ получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для несанкционированного доступа.
   2. Программное обеспечение, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность работника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям политики парольной защиты.
   3. Настройка доступа ко всем информационным ресурсам банка должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.
   4. Если система контроля доступа АРМ, корпоративной сети или автоматизированной системе вышла из строя, то по умолчанию доступ пользователей должен быть запрещен.
   5. Доступ к информационным ресурсам банка должен осуществляться согласно разработанной и утвержденной руководителем «Матрицы доступа», составленной на основании должностных обязанностей работников банка и отчета о проведенной внутренней проверки.
   6. Любое изменение в правах доступа к информационным ресурсам банкадолжно быть обосновано выполнением должностных обязанностей, утверждено и направлено администратору информационной безопасности.
   7. При увольнении работников банка или изменении их должностных обязанностей, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в трехдневный срок, после чего внести соответствующие изменения в систему контроля доступа и «Матрицу доступа».
   8. Для установления персональной ответственности идентификатор учетной записи пользователя в любой информационной системе должен однозначно соответствовать отдельному работнику.
   9. Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы или с запирающим механизмом экрана или клавиатуры, управляемым паролем, маркером или подобным механизмом аутентификации пользователя, когда они находятся без присмотра, и должны быть защищены блокировкой клавиатуры, паролями или другими средствами управления, когда не используются.
   10. Для доступа к АРМ и корпоративной сети банка у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц.
       1. Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов банка запрещено.
       2. При предоставлении идентификатора учетной записи сторонним организациям необходимо заключение соглашений, подтверждающих обязательства сторонних организаций соблюдать требования НПА РБ и организационно-распорядительных документов банка подписанные уполномоченными лицами.
       3. При прекращении необходимости использования сторонними организациям идентификатора учетной записи, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в однодневный срок, после чего должны быть внесены соответствующие изменения в систему контроля доступа и «Матрицу доступа».
       4. Для всех лиц, не являющихся служащими банка но для выполнения, обязательств которых, необходимо предоставление доступа к АРМ и корпоративной сети банка должен быть сформирован идентификатор учетной записи, действующий только на период выполнения лицом своих обязательств. В случае, если срок выполнения обязательств не определен, то срок действия идентификатора учетной записи должен составлять 60 дней.
       5. Пользователям запрещено использование идентификаторов учетных записей и паролей, используемых для получения доступа к информационным ресурсам банка, для идентификации и аутентификации на публичных ресурсах сетей общего пользования.
   11. Все автоматизированные системы и технические средства должны поддерживать специальный тип учетной записи, позволяющий производить любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности.
       1. Количество таких типов учетных записей должно быть максимально ограничено и предоставлено только тем пользователям, которым это необходимо для осуществления должностных обязанностей с учетом соблюдения требований НПА РБ и организационно-распорядительных документов банка.
       2. Таким лицам должны быть предоставлены как минимум два типа учетных записей, одна – специальный тип учетной записи, другая – ограниченный тип учетной записи для повседневной работы, не требующей изменения настроек АС.
       3. Удаленное администрирование любых технических устройств в корпоративной сети банка, при котором осуществляется передача информации через сети общего пользования, запрещено.
   12. АРМ должны переводиться в режим запроса пароля после определенного периода бездействия или при отсутствии возможности контроля пользователем доступа к АРМ.
       1. При наличии технической возможности, средства контроля доступа должны быть настроены на временную блокировку доступа к ним, после трехкратной попытки получения доступа, и уведомления уполномоченных лиц о таковых фактах.
       2. При наличии технической возможности удаленные подключения к автоматизированной системе должны автоматически отключаться после определенного времени неактивности такого подключения.
   13. Пользователям запрещено собирать и копировать информацию с информационных ресурсов, если это не обусловлено выполнением должностных обязанностей. При наличии технической возможности используемые системы контроля доступа должны предупреждать возможность таких действий и информировать о таких попытках.
   14. Программисты и другой технический персонал не должны устанавливать и использовать программное обеспечение, направленное на обход установленных механизмов доступа или получение сведений для несанкционированного доступа. Если использование такого программного обеспечения необходимо для выполнения должностных обязанностей, то его использование должно осуществляться только уполномоченными лицами.
2. **Политика обеспечения сетевой безопасности**
   1. Конфигурация и настройка всех устройств, подключенных к корпоративной сети банка должны соответствовать требованиям НПА РБ и организационно-распорядительным документам банка.
   2. Размещение в корпоративной сети банка информации ограниченного доступа должно соответствовать требованиям НПА РБ и организационно-распорядительным документам банка.
   3. Используемые внешние интерфейсы и протоколы корпоративной сети банка должны быть максимально ограничены необходимыми для обеспечения выполнения своих задач и функций.
   4. Технические средства, обеспечивающие работу корпоративной сети, должны размещаться с соблюдением требований по контролю физического доступа к ним и организации их сохранности. Доступ в помещения лиц, не уполномоченных для работы с данным оборудованием, должен быть исключен или осуществляться в сопровождении уполномоченных работников банка.
   5. Для управления техническими устройствами в сети по возможности должны быть использован протоколы поддерживающие криптографическую защиту информации.
3. **Политика использования программного обеспечения**
   1. Программное обеспечение, используемое для осуществления деятельности структурных подразделений банка должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Любое структурное подразделение банка должно исключить случаи хранения и/или использования программного обеспечения, не являющегося лицензионным.
   2. В случае если в НПА РБ предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения уполномоченными организациям и т.п.) структурное подразделение банка обязано обеспечить выполнение подобных требований.
   3. На каждое АРМ должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.
   4. Банк предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения должностных обязанностей.
   5. На технические средства, подключаемые к корпоративной сети банка и подразумевающие возможность установки программного обеспечения, должно быть установлено базовое программное обеспечение, предусмотренное «Перечнем программного обеспечения, разрешенного к установке на технических средствах, подключаемых к корпоративной сети банка.

**9. Политика парольной защиты**

* 1. Доступ к программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и/или разграничение полномочий без использования пароля запрещено.
  2. Пароли доступа к различному прикладному программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к автоматизированному рабочему месту или элементам сетевой инфраструктуры и не должны совпадать для различного программного обеспечения.
  3. Создание пароля должно предусматривать создание первичного пароля администратором, с последующей его сменой пользователем при первом запуске программного обеспечения. В случае если данная возможность не поддерживается программным обеспечением, пользователь обязан самостоятельно создать пароль пользователя при первом запуске программного обеспечения.
  4. Пароли не должны передаваться в электронных сообщениях или любых иных формах электронного обмена.
  5. Системные пароли (например, пароль учетной записи Root, администратор, а также пароли, обеспечивающие возможность полного управления и настройки (включая изменения прав доступа) используемым в банке программным обеспечением) должны меняться регулярно, но не реже одного раза в три месяца.
  6. В случае компрометации пароля необходимо его немедленное изменение, а также оповещение о данном факте администратора информационной безопасности.
  7. Внеплановая смена паролей пользователя производится в случае прекращения или изменения его полномочий (переход на другую работу внутри банка и т.п.) немедленно после окончания последнего сеанса работы данного пользователя с системой.
  8. Полная внеплановая смена всех системных паролей и паролей пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри банка и т.п.) любого из лиц, выполнявших должностные обязанности администратора и/или имевшего доступ к таким паролям.
  9. Пользователи не должны сообщать свои пароли третьим лицам, включая руководителей и лиц, осуществляющих сопровождение программного обеспечения. Администраторы автоматизированных систем не должны просить пользователей сообщить им их пароли.
  10. Хранение паролей администраторами (в том числе администраторами информационной безопасности), допускается при применении средств криптографической защиты, при этом хранение не зашифрованных системных паролей в электронном виде – запрещено. Использование администраторами функций программного обеспечения, позволяющих исключить ввод пароля при повторных запусках, возможно в исключительных случаях (например, в системе резервного копирования, системе антивирусной защиты).

**10. Политика антивирусной защиты**

* 1. Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов корпоративной сети банка на всех АРМ отдельно стоящих и подключенных к корпоративной сети и на всех портативных компьютерах.
  2. Не допускается изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате действия которых уменьшается эффективность работы АС.
  3. Обновления баз системы антивирусной защиты должно производиться регулярно. Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания.
  4. Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками банка.
  5. Структурные подразделения банка обязаны проводить сканирование своих информационных ресурсов, а также всех подключенных АРМ на наличие компьютерных вирусов и/или вредоносных программ.
  6. Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.
  7. В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, не поддерживаемые системой антивирусной защиты, файлы прошли криптографическое преобразование и т.п.), необходимо на АРМ, не подключенном к корпоративной сети багка привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.
  8. Все файлы, передаваемые третьим лицам должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи.
  9. Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандирования или распространения пользователями компьютерных вирусов или вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности автоматизированных систем банка запрещены.
  10. В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан прекратить работу и сообщить об этом администратору информационной безопасности.
  11. О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на АРМ или портативном компьютере, подключаемом к корпоративной сети банков должно быть сообщено администратору информационной безопасности.
  12. Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

**11. Политика использования отчуждаемых носителей**

* 1. Использование личных отчуждаемых носителей информации запрещено для всех работников банка. На АРМ пользователей программно-аппаратными средствами должен быть ограничен доступ к отчуждаемым носителям информации.
  2. Работники, которым необходимо использование отчуждаемых носителей информации для выполнения должностных обязанностей, должны быть обеспеченыбанкатакими носителями.
  3. Служебные отчуждаемые носители информации должны подлежать учету, а их передача работникам должна быть подтверждена их росписью. Работник несет персональную ответственность за их сохранность. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными отчуждаемыми носителями информации.
  4. Использование отчуждаемых носителей информации для хранения информации ограниченного доступа должно соответствовать требованиям НПА РБ и внутренних документов банка.
  5. Использование служебных отчуждаемых носителей информации в личных целях запрещено.
  6. Подключение служебных отчуждаемых носителей информации к техническим средствам, заведомо содержащим вирусы и/или вредоносные программы, запрещено. В этом случае отчуждаемые носители передаются администратору информационной безопасности.
  7. Эксплуатация отчуждаемых носителей информации должна осуществляться в соответствии с требованиями по их эксплуатации, и направлена на предупреждение их неисправности.

**12. Политика использования средств криптографической защиты**

* 1. Деятельность со средствами криптографической защиты должны исключать нарушение законодательства Республики Беларусь в области лицензирования. В случае, если предполагаемая деятельность со средствами криптографической защиты подразумевает необходимость получения лицензии, то банк обязан получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.
  2. При использовании средств криптографической защиты для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям НПА РБ.
  3. Установка, настройка и техническое сопровождение средств криптографической защиты должно осуществляться квалифицированными специалистами и не нарушать требования НПА РБ.
  4. Использование, в том числе хранение, средств криптографической защиты должно отвечать требованиям законодательства Республики Беларусь.
  5. Перед использованием средств криптографической защиты работники обязаны пройти обучение по порядку их использования.
  6. Пользователям запрещено использование средств криптографической защиты других пользователей, в том числе с целью выдать себя за другого пользователя.
  7. Все действия по обеспечению сохранности ключей должны быть направлены на исключение компрометации ключей.
  8. В случае компрометации ключей или подозрения на компрометацию пользователь обязан прекратить любое использование средств криптографической защиты и незамедлительно сообщить о данном факте уполномоченному лицу банка.

**13. Политика работы с бумажными носителями и работы с фотокопировальными устройствами**

* 1. Конфиденциальная информация, например, на бумажном или на электронном носителе, должна быть заперта (в сейфе, в шкафу или на полках в специальном помещении для хранения), если она не требуется, особенно в нерабочее время.
  2. Пункты работы с входящей и исходящей почтой и факсимильные аппараты, находящиеся без присмотра, должны быть защищены.
  3. Неразрешенное использование фотокопировальных устройств и другой техники воспроизведения (например, сканеры, цифровые камеры), должно предотвращаться.
  4. Документы, содержащие конфиденциальную информацию, должны удаляться с принтеров немедленно.

**14. Кадровая политика**

* 1. Претендентам на работу не должна раскрываться информация об имеющейся системе защиты информации.
  2. До начала выполнения своих должностных обязанностей до претендента должна быть доведена вся необходимая информация и проведены все инструктажи в соответствии с требованиями НПА РБ и организационно-распорядительной документации банка.
  3. Ответственное выполнение требований по информационной безопасности является обязанностью всех работников банка. Требования по информационной безопасности касаются всех работников банка.
  4. Для выполнения требований по информационной безопасности работники должны знать требования НПА РБ и организационно-распорядительной документации банка, регламентирующие данные требования и письменно подтверждать свое согласие на их выполнение.
  5. В зависимости от должностных обязанностей, знание требований по информационной безопасности могут быть включены в программу проведения аттестации персонала.
  6. Не выполнение требований НПА РБ и организационно-распорядительной документации банка, по защите информации является поводом для проведения служебных расследований и возможному привлечению к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Республики Беларусь и административно-правовыми нормами, установленными в банке.
  7. При увольнении или прекращении договорных обязательств работники должны быть уведомлены и согласны с требованиями по неразглашению информации ограниченного доступа и сведений о системе защиты информации в банке в соответствии с НПА РБ и организационно-распорядительной документацией банка.

**15. Система защиты персональных данных**

* 1. Система защиты персональных данных (СЗПДн), строится на основании:
* Перечня персональных данных, подлежащих защите;
* Акта классификации информационной системы персональных данных;
* Модели угроз безопасности персональных данных;
  1. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн . На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, и Акта о результатах проведения проверки делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.
  2. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:
* АРМ пользователей;
* Сервера приложений;
* СУБД;
* Граница ЛВС;
* Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.
  1. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:
* антивирусные средства для рабочих станций пользователей и серверов;
* средства межсетевого экранирования;
* средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.
  1. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:
* управление и разграничение доступа пользователей;
* регистрацию и учет действий с информацией;
* обеспечение целостности данных;
* обнаружение вторжений.
  1. Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителембанка или лицом, ответственным за обеспечение защиты ПДн.

**16. Требования к подсистемам СЗПДн**

* 1. СЗПДн включает в себя следующие подсистемы:
* управления доступом, регистрации и учета;
* обеспечения целостности и доступности;
* антивирусной защиты;
* межсетевого экранирования;
* анализа защищенности;
* обнаружения вторжений;
* криптографической защиты.
  1. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.
  2. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:
* идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
* идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
* идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
* регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;
* регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
* регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.
  1. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.
  2. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн банка, а также средств защиты при случайной или намеренной модификации.
  3. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.
  4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн банка.
  5. Средства антивирусной защиты предназначены для реализации следующих функций:
* резидентный антивирусный мониторинг;
* антивирусное сканирование;
* скрипт-блокирование;
* централизованная/удаленная установка/деинсталляция антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
* автоматизированное обновление антивирусных баз;
* ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
* автоматический запуск сразу после загрузки операционной системы.
  1. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.
  2. Подсистема межсетевого экранирования предназначена для реализации следующих функций:
* фильтрация открытого и зашифрованного (закрытого) IP-трафика;
* фиксация во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
* идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ;
* регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы;
* контроль целостности своей программной и информационной части;
* фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
* регистрация и учет запрашиваемых сервисов прикладного уровня;
* блокирование доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами устойчивыми к перехвату;
* контроля за сетевой активностью приложений и обнаружения сетевых атак.
  1. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.
  2. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.
  3. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.
  4. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.
  5. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.
  6. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Учреждения, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.
  7. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

**17. Пользователи ИСПДн**

* 1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.
  2. В ИСПДн банка можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:
* Администратора ИСПДн;
* Администратора информационной безопасности (ИБ);
* Оператора АРМ;
* Администратора корпоративной сети (КС);
* Технического специалиста по обслуживанию периферийного оборудования;
* Программист-разработчик ИСПДн.
  1. Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.
  2. Администратор ИСПДн – работник банка, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (АРМ) к элементам, хранящим персональные данные.
     1. Администратор ИСПДн обладает следующим уровнем доступа и знаний:
* обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
* обладает полной информацией о технических средствах и конфигурации ИСПДн;
* имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
* обладает правами конфигурирования и административной настройки технических средств ИСПДн.
  1. Администратор информационной безопасности - работник банка, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент СЗПДн.
     1. Администратор информационной безопасности обладает следующим уровнем доступа и знаний:
* обладает правами Администратора ИСПДн;
* обладает полной информацией об ИСПДн;
* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
  1. Оператор АРМ - работник банка, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.
  2. Администратор корпоративной сети - работник банка, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.
  3. Технический специалист по обслуживанию - работник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.
  4. Программисты-разработчики – разработчики прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как работники Учреждения, так и работники сторонних организаций.

**18. Требования к персоналу по обеспечению защиты ПДн**

* 1. Все работники банка являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.
  2. При вступлении в должность нового работника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.
  3. Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.
  4. Работники банка, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.
  5. Работники банка, должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
  6. Работники банка должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
  7. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
  8. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения, третьим лицам.
  9. При работе с ПДн в ИСПДн работники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
  10. При завершении работы с ИСПДн работники обязаны защитить АРМ или терминалы c помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
  11. Работники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.
  12. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

**19. Полномочия и обязанности по обеспечению информационной безопасности**

* 1. В рамках деятельности по обеспечению информационной безопасности указанные ниже работники и подразделения банка выполняют следующие функции:

Таблица 19.1 – Функции по обеспечению информационной безопасности

|  |  |
| --- | --- |
| **Работник/Подразделение** | **Функции по обеспечению информационной безопасности** |
| **Главный редактор банка** | общее руководство обеспечением информационной безопасности банка, организация своевременного и качественного обучения и проверки знаний по информационной безопасности в целом |
| **Администраторы информационной безопасности** | поддержание и совершенствование системы обеспечения информационной безопасности;  управление планами по обеспечению информационной безопасности;  разработка документов по обеспечению информационной безопасности, а также контроль исполнения данных документов; определение требований к защитным мерам |

Продолжение таблицы 19.1

|  |  |
| --- | --- |
|  | определение требований к защитным мерам обеспечения информационной безопасности;  контроль уровня информационной безопасности банка;  контроль уровня информационной безопасности банка;  расследование событий, связанных с инцидентами информационной безопасности и в случае необходимости вынесение предложений по применению санкций в соответствии с законодательством РБ в отношении лиц, осуществивших противоправные действия;  контроль своевременности обучения по информационной безопасности сотрудников банка |
| **Операторы автоматизированного рабочего места** | внедрение и эксплуатация защитных мер системы информационной безопасности;  организация мероприятий по обеспечению информационной безопасности;  контроль за соблюдением требований информационной безопасности |
| **Руководители структурных подразделений банка** | соблюдение принципа минимальности при предоставлении доступа к информационным активам и компонентам информационной инфраструктуры;  ознакомление с документами и требованиями по обеспечению информационной безопасности работников возглавляемых подразделений;  организация своевременного и качественного обучения и проверки знаний по информационной безопасности в структурных подразделениях;  выполнение работниками возглавляемого подразделения требований и правил банка по обеспечению информационной безопасности |
| **Работник банка** | соблюдение требований законодательных и нормативных документов, в том числе внутренних нормативных документов банка по вопросам информационной безопасности;  соблюдение прав банка на информационные активы, информационную инфраструктуру и интеллектуальную собственность;  своевременное уведомление непосредственных руководителей, ответственного работника и управления информационной безопасности о фактических или потенциально возможных интеллектуальную собственность; своевременное уведомление непосредственных |

Продолжение таблицы 19.1

|  |  |
| --- | --- |
|  | руководителей, ответственного работника и управления информационной безопасности о фактических или потенциально возможных инцидентах информационной безопасности, угрозах и уязвимости, а также о несанкционированных действиях и обращениях неуполномоченных лиц |

**20. Ответственность работников ИСПДн издательства**

* 1. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.
  2. При нарушениях пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Республики Беларусь.
  3. Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях работников банка.
  4. Все работники банка в соответствии с законодательством Республики Беларусь несут дисциплинарную и материальную ответственность за неисполнение или ненадлежащее исполнение требований по обеспечению информационной безопасности, определенных Политикой и иными внутренними документами банка.
  5. Требования настоящей Политики распространяются на всех работниковбанка**,** а также всех прочих лиц, допущенных к работам.

**21. Оценка рисков**

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

Таблица 21.1 - Численная шкала для оценки ущерба издательству от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 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 |

Продолжение таблицы 21.1

|  |  |
| --- | --- |
| 3 | Значительные потери на рынке и в прибыли. От издательства 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 |

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

Таблица 21.1 - Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| 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 |

* 1. В рамках деятельности по обеспечению информационной безопасности оценка рисков следующая:

Таблица 21.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб x Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Межсайтовое кодирование (XSS-атаки) | 2 | 0,1 | 0,2 |
| SQL-инъекции | 2 | 0,1 | 0,2 |
| Вирусы | 2 | 0,1 | 0,2 |
| DDoS-атаки | 2 | 0,1 | 0,2 |
| Неправильная конфигурация web-сервера | 1 | 0,1 | 0,1 |
| Пиратское ПО | 3 | 0,1 | 0,3 |
| Атака типа man-in-the-middle | 4 | 0.3 | 0.5 |
| IP-спуфинг | 4 | 0.3 | 0.5 |
| Итого | 14 | 1,1 | 2,9 |

**Вывод**

В ходе работы мы вывели список возможных опасностей, которые могут произойти с информацией учреждения. 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.

И, наконец, устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. Если происходит инцидент, связанный с нарушением безопасности, или система дает сбой в работе, политики и процедуры устанавливают порядок действий и выполняемые задачи, направленные на устранение последствий этого инцидента.

Также из вышесказанного в работе следует, что при разработке политики информационной безопасности учреждения, в том числе и школы, 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.