Учреждение образования

«Белорусский Государственный Технологический Университет»

Кафедра программной инженерии

Разработка политики информационной

безопасности издательства

Выполнил: студент 3 курса 6 группы ФИТ

Капорцев Олег

Минск 2021

**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**

Целью настоящей политики является обеспечение безопасности объектов защиты ИСПДн издательства от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в перечне персональных данных обрабатываемых в издательстве.

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

Основными целями обеспечения ИБ являются:

* соответствие требованиям законодательства, требованиям надзорных и регулирующих органов;
* повышение стабильности функционирования издательства в целом;
* достижение адекватности мер по защите от реальных угроз информационной безопасности;
* предотвращение и/или снижение ущерба от инцидентов информационной безопасности;
* повышение доверия к издательству со стороны клиентов, контрагентов, партнеров, инвесторов и общественности в целом, повышение рейтинга издательства и его инвестиционной привлекательности;
* защита законных прав издательства 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;

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**

Автоматизированная система обработки информации издательства является распределенной структурой, объединяющей в единую ИС подсистемы центрального аппарата, региональных филиалов. Основными объектами обеспечения информационной безопасности в издательства признаются следующие элементы:

* информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством к государственной тайне, коммерческой тайне издательства, открытая информация, необходимая для обеспечения нормального функционирования издательства (в дальнейшем - защищаемая информация);
* средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
* программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы издательства, с помощью которых производится обработка защищаемой информации;
* помещения, предназначенные для ведения закрытых переговоров и совещаний;
* помещения, в которых расположены средства обработки защищаемой информации;
* технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может находиться:

* на бумажных носителях;
* электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
* передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
* в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
* записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны и др.).

**4. Угрозы информационной безопасности**

* 1. **Угрозы конфиденциальности (неправомерный доступ к информации).**

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств.

* 1. **Угрозы целостности (неправомерное изменение данных).**

Угрозы нарушения целостности — это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности, может быть, вызвано различными факторами — от умышленных действий персонала до выхода из строя оборудования.

* 1. **Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).**

Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

**5. Источники угроз информационной безопасности**

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Группа угроз, обусловленная действиями субъекта (антропогенные источники) — субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними, так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.

Группа угроз, обусловленная техническими средствами (техногенные источники) — эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними.

Стихийные источники — данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

1. **Оценка угроз, рисков и уязвимостей**

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

Таблица 6.1 - Численная шкала для оценки ущерба издательству от НСД

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

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

Таблица 6.2 - Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 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 |

В рамках деятельности по обеспечению информационной безопасности оценка рисков следующая:

Таблица 6.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб x Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Утечка продуктов | 3 | 0,2 | 0,6 |
| Взлом базы данных | 3 | 0,1 | 0,3 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Вирусы | 1 | 0,2 | 0,2 |
| Пиратское ПО | 1 | 0,1 | 0,1 |
| Итого |  | 1 | 2,2 |

1. **Политика обеспечения сетевой безопасности**

Конфигурация и настройка всех устройств, подключенных к корпоративной сети издательства должны соответствовать требованиям НПА РБ и организационно-распорядительным документам издательства.

Размещение в корпоративной сети издательства информации ограниченного доступа должно соответствовать требованиям НПА РБ и организационно-распорядительным документам издательства.

Используемые внешние интерфейсы и протоколы корпоративной сети издательства должны быть максимально ограничены необходимыми для обеспечения выполнения своих задач и функций.

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 издательства.

Для управления техническими устройствами в сети по возможности должны быть использован протоколы поддерживающие криптографическую защиту информации.

1. **Политика использования программного обеспечения**

Программное обеспечение, используемое для осуществления деятельности структурных подразделений издательства 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 издательства должно исключить случаи хранения и/или использования программного обеспечения, не являющегося лицензионным.

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 издательства обязано обеспечить выполнение подобных требований.

На каждое АРМ должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.

Издательство предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения должностных обязанностей.

На технические средства, подключаемые к корпоративной сети издательства 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 издательства.

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

Все работники издательства, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн. 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. Работники издательства, 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. Пароли не должны передаваться в электронных сообщениях или любых иных формах электронного обмена.

Работники издательства, 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.

Работники издательства должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники издательства должны обеспечивать надлежащую защиту оборудования, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационной системой издательства, третьим лицам.

Работники обязаны сообщать обо всех случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и/или лицу, отвечающему за защиту персональных данных в ИСПДн.

**10. Политика антивирусной защиты**

Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов корпоративной сети издательства на всех АРМ отдельно стоящих и подключенных к корпоративной сети и на всех портативных компьютерах.

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.

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.

Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками издательства.

Структурные подразделения издательства обязаны проводить сканирование своих информационных ресурсов, а также всех подключенных АРМ на наличие компьютерных вирусов и/или вредоносных программ.

Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.

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 издательства привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.

Все файлы, передаваемые третьим лицам должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи.

Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандированное или распространения пользователями компьютерных вирусов или вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности автоматизированных систем издательства запрещены.

В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан прекратить работу и сообщить об этом администратору информационной безопасности.

О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на АРМ или портативном компьютере, подключаемом к корпоративной сети издательств должно быть сообщено администратору информационной безопасности.

Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

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

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.

Пункты работы с входящей и исходящей почтой и факсимильные аппараты, находящиеся без присмотра, должны быть защищены.

Неразрешенное использование фотокопировальных устройств и другой техники воспроизведения (например, сканеры, цифровые камеры), должно предотвращаться.

Документы, содержащие конфиденциальную информацию, должны удаляться с принтеров немедленно.

**12. Система защиты персональных данных**

Система защиты персональных данных (СЗПДн), строится на основании:

* Перечня персональных данных, подлежащих защите;
* Акта классификации информационной системы персональных данных;
* Модели угроз безопасности персональных данных;

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.

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.

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.

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.

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 руководителемиздательства или лицом, ответственным за обеспечение защиты ПДн.

**13. Требования к подсистемам СЗПДн**

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.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

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.

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.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн издательства, а также средств защиты при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн издательства.

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.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

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.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

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.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

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

В рамках деятельности по обеспечению информационной безопасности указанные ниже работники и подразделения издательства выполняют следующие функции:

Таблица 14.1 – Функции по обеспечению информационной безопасности

|  |  |
| --- | --- |
| **Работник/Подразделение** | **Функции по обеспечению информационной безопасности** |
| **Руководитель издательства** | Общее руководство обеспечением информационной безопасности издательства, 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 обеспечения информационной безопасности;  Контроль уровня информационной безопасности издательства;  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 издательства |
| **Операторы автоматизированного рабочего места** | Внедрение и эксплуатация защитных мер системы информационной безопасности;  Организация мероприятий по обеспечению информационной безопасности;  Контроль за соблюдением требований информационной безопасности |

14.1. Продолжение таблицы

|  |  |
| --- | --- |
| **Руководители структурных подразделений издательства** | 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 издательства по обеспечению информационной безопасности |
| **Работник издательства** | Соблюдение требований законодательных и нормативных документов, в том числе внутренних нормативных документов издательства по вопросам информационной безопасности;  Соблюдение прав издательства на информационные активы, информационную инфраструктуру и интеллектуальную собственность;  Своевременное уведомление непосредственных 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 |

**15. 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.