Утверждаю:
директор МБОУ г. Астрахань «СОШ №51»
_____И.В. Загоруйко

Частная модель угроз безопасности персональных данных для информационных систем персональных данных

Муниципальное бюджетное образовательное учреждение
г. Астрахани «Средняя образовательная школа №51»

414018, г. Астрахань, ул. Адмирала Нахимова, д.44

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в информационных системах персональных данных, принадлежащих Муниципальному бюджетному общеобразовательному учреждению г. Астрахани «Средняя общеобразовательная школа №51» (далее – Школа), расположенных по адресу:414018, г. Астрахань, ул. Адмирала Нахимова, д. 44,строится на основании следующих документов:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

В модели угроз представленыхарактеристики информационных систем персональных данных(ИСПДн)Школы, состав и режим обработки персональных данных(ПДн), классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных (УБПДн).

СОКРАЩЕНИЯ

АС – автоматизированная система
ИСПДн – информационная система персональных данных
НСД – несанкционированный доступ к информации
ПДн – персональные данные
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
СВТ – средства вычислительной техники
СЗИ – средство защиты информации
СЗПДн – система защиты персональных данных
УБПДн – угрозы безопасности персональных данных
ФСТЭК России – Федеральная служба по техническому и экспортному контролю

1. ТЕРМИНЫ И 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.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

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.

Блокирование персональных данных– временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

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

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных(ИСПДн) – это 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.

Информационные технологии– процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

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

Межсетевой экран– локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им посвоим функциональному предназначению и техническим характеристикам.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – 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.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. ОПИСАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Информационные системы персональных данных Школы предназначены для поддержки технологических процессов работы Школы.

Информационные системы персональных данных Школы позволяют осуществлять коммерческую деятельность, вести бухгалтерский и кадровый учет, учет административно-хозяйственной деятельности, формировать различные внутренние отчеты.

Рассматриваемые ИСПДнШколы имеют подключение к сетям общего пользования и международного обмена.

Обработка персональных данных в ИСПДнШколы ведется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение (передача, предоставления), обезличивание, блокирование, удаление, уничтожение персональных данных.

Описание информационной системы АРМ "ФИС ФРДО"

Информационная система развёрнута на одном компьютере. Компьютер имеет выход в сеть Интернет. Обработка персональных данных осуществляется в программе «MicrosoftOffice» и на портале ФИС ФРДО. Персональные данные предаются в Министерство образования и науки Астраханской области.

Описание информационной системы АРМ "Бухгалтерия"

Информационная система развёрнута на четырех компьютерах. Компьютеры имеют подключение к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «MicrosoftOffice», «1С:Предприятие», «СБИС». Персональные данные передаются в Астраханское региональное отделение Фонда социального страхования РФ, Управление пенсионного фонда России в Советском районе г. Астрахани, Межрайонную инспекцию Федеральной налоговой службы № 6 по Астраханской области, Управление Федеральной службы государственной статистики по Астраханской области и Республике Калмыкия.

Описание информационной системы АРМ "АИС: Зачисление"

Информационная система развёрнута на одном компьютере. Компьютер имеет выход в сеть Интернет. Обработка персональных данных осуществляется в программах «MicrosoftOffice», «АИС: Зачисление». Персональные данные передаются в Управление образования администрации муниципального образования г. Астрахань.

Описание информационной системы "Сайт"

Информационная система представляет собой официальный сайт Администрации с доменным именем https://sosh51.nubex.ru/. Общедоступная информация о деятельности

Школы, предоставляется неограниченному кругу лице посредством ее размещения в сети Интернет. Сайт размещен на виртуальном хостинге NUBEX.RU, датацентр расположен на территории Российской Федерации в городе Москва. Используется небезопасный протокол HTTPS, что исключает возможность перехвата сессии легального пользователя и проведения атаки «человек посередине».

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что информационным системам персональных данных Школы необходимо обеспечить 4 уровень защищенности.

Все компоненты ИСПДнШколы расположены в пределах контролируемой зоны и находятся на территории Российской Федерации.

3. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

3.1. Классификация возможных нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

1. Внешние нарушители – физические лица, не имеющие права пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн;
2. Внутренние нарушители – физические лица, имеющие право пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн.

3.1.1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Потенциально внешними нарушителями для ИСПДн могут быть:

1. Разведывательные службы государств;
2. Криминальные структуры;
3. Конкуренты (конкурирующие организации);
4. Недобросовестные партнеры;
5. Внешние субъекты (физические лица).

Внешние нарушители имеют возможности:

1. Воздействовать на защищаемую информацию по техническим каналам утечки информации;
2. Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
3. Осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и сетям международного информационного обмена;
4. Осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
5. Осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
6. Осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Исходя из особенностей функционирования ИСПДнШколы, объема и критичности сведений, обрабатываемых в ней, список потенциальных нарушителей был сокращен до следующего:

1. Криминальные структуры;
2. Внешние субъекты (физические лица).

Предполагается, что выявленные внешние нарушители не могут получать доступ к защищаемой информации и воздействовать на нее по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешних нарушителей к осуществлению указанных действий.

Таким образом, выявленные внешние нарушители могут воздействовать на защищаемую информацию всеми перечисленными выше способами, за исключением действий, направленных на утечку и искажение конфиденциальной информации по техническим каналам.

3.1.2. Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- пользователи ИСПДн (категория II);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИСПДн, но не имеющие права доступа к ресурсам (категория III);
- обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория IV);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория V).

На лиц I категории возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к

защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

На лиц II категории возложены задачи по использованию программно-аппаратных средств и баз данных ИСПДн. Пользователи потенциально могут реализовывать угрозы ИБ используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-V относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

3.2. Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:

1. Общая информация – информация о назначениях и общих характеристиках ИСПДн;
2. Эксплуатационная информация – информация, полученная из эксплуатационной документации;
3. Чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

1. Данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
2. Сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
3. Данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
4. Данные о реализованных в СЗИ принципах и алгоритмах;
5. Сведения о возможных каналах реализации угроз;
6. Информацию о способах реализации угроз.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в Школе конкретные организационные меры и компетенцию нарушителей.

В связи с изложенным, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз.

3.3. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель **имеет**:

1. Аппаратные компоненты ИСПДн и СЗИ;
2. Доступные в свободной продаже технические средства и программное обеспечение;
3. Специально разработанные технические средства и программное обеспечение.
4. Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные в Школе конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Так как специальные средства, используемые для реализации угроз утечки информации по техническим каналам, отсутствуют в свободной продаже, предполагается, что потенциальные нарушители **не имеют**:

1. Средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ) на ИСПДн;
2. Средств воздействия на источники питания и через цепи питания;
3. Средств воздействия через цепи заземления;
4. Средств активного воздействия на технические средства (средств облучения).

Предполагается, что нарушитель обладает совершенными средствами реализации угроз.

4. УГРОЗЫИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Угрозы от утечки по техническим каналам

4.1.1. Угроза утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

На территории Школы введен контроль доступа в контролируемую зону. В ИСПДнШколыотсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.

Вероятность реализации угрозы – **маловероятна**.

4.1.2. Угроза утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

На территории Школы введен контроль доступа в контролируемую зону. На окнах установлены жалюзи. Большая часть окон выходит во двор контролируемой зоны, что практически исключает визуальный просмотр посторонними лицами информации на мониторе.

Вероятность реализации угрозы – **маловероятна**.

4.1.3. Угроза утечки информации по каналам ПЭМИН

Возникновение угрозыПДнпо каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Реализация угроз по каналам ПЭМИН требует высоких затрат и специальных средств. Предположительно, вероятный нарушитель не обладает такими средствами.

Вероятность реализации угрозы – **маловероятна**.

4.2. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

4.2.1. Угрозы уничтожения, хищения аппаратных средств информационной системы носителей информации путем физического доступа к элементам информационной системы

4.2.1.1. Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

На территории Школы введен контроль доступа в контролируемую зону. На входе постоянно дежурят сотрудники охраны. Установлены система видеонаблюдения, охранная сигнализация, тревожные кнопки.

Вероятность реализации угрозы – **маловероятна**.

4.2.1.2. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

На территории Школы введен контроль доступа в контролируемую зону. На входе постоянно дежурят сотрудники охраны. Установлены система видеонаблюдения, охранная сигнализация, тревожные кнопки.

Вероятность реализации угрозы – **низкая**.

4.2.1.3. Кража паролей доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

На территории Школы введен контроль доступа в контролируемую зону. На входе постоянно дежурят сотрудники охраны. Установлены система видеонаблюдения, охранная сигнализация, тревожные кнопки. Утверждена инструкция по организации парольной защиты, запрещающая хранение паролей доступа на бумажных или электронных носителях без соответствующей защиты от несанкционированного доступа к ним.

Вероятность реализации угрозы – **низкая**.

4.2.1.4. Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

На территории Школы введен контроль доступа в контролируемую зону. Утверждена разрешительная система доступа (организационная мера) к информационным ресурсам.

Вероятность реализации угрозы – **низкая**.

4.2.1.5. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

На территории Школы введен контроль доступа в контролируемую зону.

Вероятность реализации угрозы – **низкая**.

4.2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В Школетехническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

На территории Школы введен контроль доступа в контролируемую зону. Техническое обслуживание узлов ПЭВМ осуществляется сотрудниками Школы, которые подписали обязательство о неразглашении конфиденциальной информации.

Вероятность реализации угрозы – **маловероятна**.

4.2.1.7. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

На территории Школы введен контроль доступа в контролируемую зону. Пользователи работают под ограниченными учетными записями. Утверждены инструкция пользователя ИСПДн и инструкция по антивирусной защите.

Вероятность реализации угрозы – **маловероятна**.

4.2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

4.2.2.1. Действия вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу

(набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На компьютерах Школы установлены антивирусные программы. Утверждена инструкция по антивирусной защите.

Вероятность реализации угрозы – **низкая**.

4.2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Используются сертифицированные средства защиты.

Вероятность реализации угрозы – **маловероятна**.

4.2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПОвнутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Пользователи работают под ограниченными учетными записями. Утверждена инструкция пользователя ИСПДн, запрещающая пользователям самостоятельную установку стороннего программного обеспечения.

Вероятность реализации угрозы – **маловероятна**.

4.2.2.4. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере

Угроза осуществляется путем утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнения форм авторизации.

Утверждена инструкция по организации парольной защиты, устанавливающая правила использования и хранения паролей.На компьютерах Школы установлены антивирусные программы.

Вероятность реализации угрозы – **низкая**.

4.2.2.5. Угроза скрытной регистрации вредоносной программной учетных записей администраторов

Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере.

Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения).

Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей).

Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт.

На компьютерах Школы установлены антивирусные программы. Утверждены инструкция по антивирусной защите и разрешительная система доступа.

Вероятность реализации угрозы – **низкая**.

4.2.2.6. Угроза хищения аутентификационной информации из временных файлов cookie

Угроза заключается в возможности хищения с использованием вредоносной программы аутентификационной информации пользователей, их счетов, хранящейся во временных файлах cookie, и передачи этой информации нарушителям через открытый RDP-порт.

Данная угроза обусловлена недостаточностью мер антивирусной защиты, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения).

Кроме того, данная угроза обусловлена непринятием мер по стиранию остаточной информации из временных файлов (очистке временных файлов).

Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт.

На компьютерах Школы установлены антивирусные программы.

Вероятность реализации угрозы – **низкая**.

4.2.2.7. Угроза использования уязвимых версий программного обеспечения

Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей.

На компьютерах Школы установлены антивирусные программы. Программное обеспечение, используемое в Школе, регулярно обновляется.

Вероятность реализации угрозы – **маловероятно**.

4.2.2.8. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика

Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных.

Данная у гроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов.

Реализация данной угрозы возможна:

- при условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения;
- при отсутствии или недостаточной реализации мер межсетевого экранирования.

На компьютерах Школы установлены антивирусные программы.

Вероятность реализации угрозы – **низкая**.

4.2.2.9. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет

Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер

антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при:

- неограниченном доступе пользователя в сеть Интернет;
- наличии у нарушителя сведений о сайтах, посещаемых пользователем.

На компьютерах Школы установлены антивирусные программы. На сетевом шлюзе настроены правила межсетевого экранирования.

Вероятность реализации угрозы – **низкая**.

4.2.2.10. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива.

Установка программного обеспечения в Школе осуществляется только с официальных дистрибутивов.

Вероятность реализации угрозы – **маловероятно**.

4.2.2.11. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы

Угроза заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему.

Данная угроза обусловлена ошибками в процессорах (например, ошибками в процессоре Intel поколения Haswell), позволяющими за счет создания специальных приложений осуществлять обход механизмов защиты, встроенных в операционную систему (например, механизма ASLR).

Реализация данной угрозы возможна при: инициировании коллизии в таблице целевых буферов - с ее помощью можно узнать участки памяти, где находятся конкретные фрагменты кода;

- создании приложения, использующего эти фрагменты кода для обхода механизма защиты;
- запуске данного приложения в связке с эксплойтом какой-либо уязвимости самой операционной системы для создания возможности удаленного запуска вредоносного кода.

На компьютерах Школы установлены антивирусные программы. Программное обеспечение, используемое в Школе, регулярно обновляется.

Вероятность реализации угрозы – **маловероятно**.

4.2.2.12. Угроза физического устаревания аппаратных компонентов

Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).

Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем.

Устаревающая компьютерная техника в Школе по возможности заменяется на новую.

Вероятность реализации угрозы – **маловероятно**.

4.2.2.13. Угроза внедрения вредоносного кода через рекламу, сервисы и контент

Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы.

Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации.

Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов в сети Интернет.

На компьютерах Школы установлены антивирусные программы. На сетевом шлюзе настроены правила межсетевого экранирования.

Вероятность реализации угрозы – **низкая**.

4.2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и системы защиты в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений) характера

4.2.3.1. Утрата паролей доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или

компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Утверждена инструкция по организации парольной защиты, устанавливающая правила использования и хранения паролей.

Вероятность реализации угрозы – **средняя.**

4.2.3.2. Непреднамеренная модификация (уничтожение) информации работниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

Пользователи работают под ограниченными учетными записями. Утверждена инструкция пользователя ИСПДн. Ежедневно осуществляется резервное копирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **низкая.**

4.2.3.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

Пользователи работают под ограниченными учетными записями.

Вероятность реализации угрозы – **маловероятно.**

4.2.3.4. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

Ежедневно осуществляется резервное копирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **низкая.**

4.2.3.5. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В Школе ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания. Ежедневно осуществляется резервное копирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **маловероятна.**

4.2.3.6. Стихийное бедствие

Угроза осуществляется вследствие возникновения природного или природно-антропогенного явления, из-за которого может происходить нарушение целостности и доступности защищаемой информации.

Ежедневно осуществляется резервное копирование ключевых элементов ИСПДн. Утверждена инструкция пользователя при возникновении внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна.**

4.2.4. Угрозы преднамеренных действий внутренних нарушителей

4.2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

На территории Школы введен контроль доступа в контролируемую зону.Утверждены разрешительная система доступа (организационная мера) к информационным ресурсам и инструкция пользователя ИСПДн.

Вероятность реализации угрозы -- **маловероятна.**

4.2.4.2. Разглашение информации, модификация, уничтожение работниками, допущенными к обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

Утверждена инструкция пользователя ИСПДн, регламентирующая работу с персональными данными. Все сотрудники подписали обязательство о неразглашении конфиденциальной информации.

Вероятность реализации угрозы – **средняя.**

4.2.5. Угрозы несанкционированного доступа по каналам связи

4.2.5.1. Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

На территории Школы введен контроль доступа в контролируемую зону, исключающий подключение злоумышленников к сегментам сети Школы на территории Школы. При передаче информации по сетям за пределы контролируемой зоны используются сертифицированные криптографические средства.

Вероятность реализации угрозы – **маловероятна.**

4.2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационной системы, топологии сети, открытых портов, служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

На сетевом шлюзе настроены правила, направленные на предотвращение данных угроз.

Вероятность реализации угрозы – **низкая.**

4.2.5.3. Угрозы выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Утверждена инструкция по организации парольной защиты, устанавливающая правила создания и частоту смены паролей.

Вероятность реализации угрозы – **низкая.**

4.2.5.4. Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

При передаче информации за пределы контролируемой зоны используются сертифицированные криптографические средства.

Вероятность реализации угрозы – **низкая.**

4.2.5.5. Угрозы подмены доверенного объекта в сети

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

При передаче информации за пределы контролируемой зоны используются сертифицированные криптографические средства.

Вероятность реализации угрозы – **низкая.**

4.2.5.6. Угрозы внедрения ложного объекта

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях NovellNetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

На сетевом шлюзе настроены правила, направленные на предотвращение данных угроз. Установлены антивирусные программы. При передаче информации за пределы контролируемой зоны используются сертифицированные криптографические средства.

Вероятность реализации угрозы – **низкая.**

4.2.5.7. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

– скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMPRedirectHost, DNS-flooding) или идентификационной и аутентификационной информации;

– явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На сетевом шлюзе настроены правила, направленные на предотвращение данных угроз. Программное обеспечение на сетевом оборудование регулярно обновляется.

Вероятность реализации угрозы – **низкая.**

4.2.5.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back.Orifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На сетевом шлюзе настроены правила, направленные на предотвращение данных угроз. Установлены антивирусные программы.

Вероятность реализации угрозы – **низкая.**

4.2.5.9. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

На сетевом шлюзе настроены правила, направленные на предотвращение данных угроз. Установлены антивирусные программы.

Вероятность реализации угрозы – **низкая.**

5. ИСХОДНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под исходным уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице1 представлены характеристики уровня исходной защищенности для ИСПДнШколы.

Таблица 1 – Характеристикиуровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**
По территориальному размещению ЛокальнаяИСПДн, развернутая в пределах одного здания	Высокий
По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
По встроенным (легальным) операциям с записями баз персональных данных Модификация, передача	Низкий
По разграничению доступа к персональным данным ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
По наличию соединений с другими базами ПДн иных ИСПДн ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
По уровню обобщения (обезличивания) ПДн ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки ИСПДн, предоставляющаячасть ПДн;	Средний

Таким образом, исходя из вышеперечисленных данных, коэффициент Y1=5

6. ОПРЕДЕЛЕНИЕ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Исходный уровень защищенности – средний (Y1=5).

Определение актуальных угроз безопасности персональных данных представлено в таблице 2.

Таблица2 – Угрозы безопасности

Угроза	Исходный уровень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
1.2. Угрозы утечки видовой информации	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
2. Угрозы несанкционированного доступа к информации						
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн						
2.1.1. Кража ПЭВМ	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.1.2. Кража носителей информации	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.1.3. Кража паролей доступа	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.1.4. Кража, модификация, уничтожение информации.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная

Угроза	Исходный уровень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.1.7. Несанкционированное отключение средств защиты	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						
2.2.1. Действия вредоносных программ (вирусов)	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.2.4. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.5.Угроза скрытной регистрации вредоносной программной учетных записей администраторов	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.6. Угроза хищения аутентификационной информации из временных файлов cookie	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.7. Угроза использования уязвимых версий программного обеспечения	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная

Угроза	Исходный уровень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
2.2.8. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.9. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.2.10. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.2.11. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.2.12. Угроза физического устаревания аппаратных компонентов	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.2.13. Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Высокая	Актуальная
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата паролей доступа	Средний (Y1=5)	Средняя (Y2=5)	Y=0,5	Средняя	Средняя	Неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.3.3. Непреднамеренное отключение средств защиты	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.3.4. Выход из строя аппаратно-программных средств	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная

Угроза	Исходный уровень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
2.3.5. Сбой системы электроснабжения	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
2.3.6. Стихийное бедствие	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Средняя	Неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средний (Y1=5)	Средняя (Y2=5)	Y=0,5	Средняя	Средняя	Актуальная
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации						
2.5.1.1. Перехват за переделами контролируемой зоны;	Средний (Y1=5)	Маловероятна (Y2=0)	Y=0,25	Низкая	Низкая	Неактуальная
2.5.2.Угроза сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.3. Угроза выявления паролей по сети.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.4. Угроза навязывание ложного маршрута сети.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная

Угроза	Исходный уровень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
2.5.5. Угроза подмены доверенного объекта в сети.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.6. Угроза внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.7. Угроза типа «Отказ в обслуживании».	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.8. Угроза удаленного запуска приложений.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная
2.5.9. Угроза внедрения по сети вредоносных программ.	Средний (Y1=5)	Низкая (Y2=2)	Y=0,35	Средняя	Низкая	Неактуальная

ЗАКЛЮЧЕНИЕ

Представленная модель угроз должна использоваться для проектирования системы защиты ИСПДнШколы.

Для предотвращения возможности реализации актуальных угроз безопасности необходимо:

- регулярно устанавливать обновления безопасности на все ключевые элементы ИСПДн (сервера, компьютеры, сетевое оборудование, средства защиты информации);
- ежедневно обновлять антивирусные базы;
- осуществлять постоянное резервирование информации, хранящейся в ИСПДн;
- периодически проводить обучение сотрудников на предмет обеспечения безопасности ПДн в Школе.

ПРИЛОЖЕНИЕ А. МЕТОДИКА РАСЧЕТА АКТУАЛЬНОСТИ

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 3.

Таблица3 –Показателиисходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределеннаяИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городскаяИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальнаяИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	**Средний**	**Низкий**
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет ***высокий*** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет ***средний*** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет ***низкую*** степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная