Муниципальное бюджетное общеобразовательное учреждение
«Средняя школа № 16 города Евпатории Республики Крым»
(МБОУ «СШ № 16»)

УТВЕРЖДЕНО
Директором школы
_____ О.А. Гонцова
Приказ № ____/01-16
от 01.09.2020 г.

МОДЕЛЬ УГРОЗ
муниципального бюджетного общеобразовательного учреждения «Средняя школа №16 города Евпатории Республики Крым»

(объект Республика Крым, г. Евпатория, ул. 60 лет ВЛКСМ д.30)

Составили:

Чернобиль Юлия Глебовна, заместитель директора по учебно- воспитательной работе муниципального бюджетного общеобразовательного учреждения «Средняя школа №16 города Евпатории Республики Крым»,
Билык Наталья Михайловна, системный администратор муниципального бюджетного общеобразовательного учреждения «Средняя школа №16 города Евпатории Республики Крым»

Ознакомлен:
Чернобиль Ю.Г.
Билык Н.М.

г. Евпатория
2020 год

Обозначения и сокращения:

- **ИСПДн** - информационная система персональных данных;
- **ндв** - недекларированные возможности;
- **нсд** - несанкционированный доступ;
- **ОС** - операционная система;
- **ПДн** - персональные данные;
- **ПО** - программное обеспечение;
- **ПЭМИН** - побочные электромагнитные излучения и наводки;
- **СВТ** - средство вычислительной техники;
- **СЗИ** - средство защиты информации;
- **СЗПДн** - система защиты персональных данных;
- **УБПДн** - угрозы безопасности персональных данных.

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;
- **автоматизированное рабочее место** - программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида;
- **аппаратные средства** - 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;
- **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;
- **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;
- **доступ к информации** - возможность получения информации и ее использования;
- **защищаемая информация** - информация, являющаяся предметом собственности, подлежащая защите в соответствии с требованиями правовых документов и (или) требованиями, устанавливаемыми собственником информации;
- **идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
- **информационная система персональных данных** - совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **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 по своим 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** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;
- **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;

- **средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
- **технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала 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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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.

ВВЕДЕНИЕ

Настоящий документ подготовлен в рамках выполнения работ по созданию СЗПДн информационных систем персональных данных управления образования администрации города Евпатории Республики Крым (далее – оператор ИСПДн).

Настоящий документ содержит модель угроз безопасности персональных данных ИСПДн (далее - модель угроз).

Разработка модели угроз является необходимым условием формирования требований к обеспечению безопасности информации ИСПДн и проектирования ИСПДн и используется для:

- анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых с использованием методов и способов защиты ПДн, предусмотренных соответствующего класса ИСПДн;
- разработки мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- разработки мероприятий по недопущению воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- планированию мероприятий по контролю обеспечения уровня защищенности персональных данных.

В процессе развития ИСПДн предполагается конкретизировать и пересматривать модель угроз для ИСПДн. Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

При разработке модели угроз для ИСПДн предусматривается, что она является специальной информационной системой ПДн, имеющей подключение к сетям связи общего пользования и (или) сетям международного информационного обмена. Обработка персональных данных в ИСПДн ведется в многопользовательском режиме с разграничением прав пользователей.

Раздел I

1. Назначение, структура и основные характеристики ИСПДн.

1.1. Рассматриваемая ИСПДн является локальной информационной системой, имеющей подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

1.2. Обработка персональных данных в ИСПДн ведется в многопользовательском режиме с разграничением прав пользователей. Режим обработки предусматривает следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, удаление.

Основные параметры ИСПДн приведены в таблице 1.

Таблица 1

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Комплексы аппаратных и программных средств, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением прав пользователей
Дополнительная информация	К персональным данным предъявляется требование конфиденциальности, целостности и доступности

1.3. В ИСПДн обрабатываются следующие типы ПДн: специальные и общедоступные.

1.4. Описание технологической и организационной структуры ИСПДн, а также состав программных и аппаратных средств ИСПДн, представлены в перечне информационных систем.

1.5. Уровни доступа пользователей к ресурсам ИСПДн представлены в регламенте по допуску сотрудников к обработке персональных данных муниципального бюджетного общеобразовательного учреждения «Средняя школа №16 города Евпатории Республики Крым»

Раздел II

2. Модель вероятного нарушителя информационной безопасности.

2.1. По признаку принадлежности к ИСПДн нарушителей можно условно разделить на две группы:

- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

2.2. 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 обеспечению высокой профессиональной подготовки кадров, допуску физических лиц 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.

К внутренним нарушителям относятся:

- лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн (Н1);
- зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места (Н2);
- зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам (Н3);
- зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн (Н4);
- зарегистрированные пользователи с полномочиями системного администратора ИСПДн (Н5);
- зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн (Н6);
- программисты-разработчики (поставщики) прикладного программного обеспечения и обеспечивающие его сопровождение на защищаемом объекте (Н7);
- разработчики и лица, обеспечивающие поставку, сопровождение и ремонт аппаратных средств на ИСПДн (Н8).

Предполагается, что лица категории Н1 могут иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн, располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) используемых коммуникационных протоколах и их сервисах, распюлагать именами и выявление паролей зарегистрированных пользователей, изменять конфигурацию аппаратных средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать информации, используя непосредственное подключение к техническим средствам ИСПДн.

Лица категории Н2 обладают всеми возможностями лиц категории Н1, знают, по меньшей мере, одно легальное имя доступа, обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн, располагают конфиденциальными данными к которым имеют доступ.

Лица категории Н3 могут обладать всеми возможностями категорий Н1 и Н2, располагают информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн, а также иметь возможность прямого (физического) доступа к фрагментам аппаратных средств ИСПДн.

На лиц категорий Н4, Н5 и Н6 возложены задачи по администрированию программных и 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 аппаратным и программным средствам ИСПДн, включая средства защиты, используемые в конкретных подсистемах и ИСПДн в соответствии с установленными для них административными полномочиями. Эти лица знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и методами безопасности. Предполагается, что они могли бы использовать стандартное оборудование для идентификации уязвимостей, либо для реализации угроз информационной безопасности. 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 внедрения устройств негласного съема информации.

К лицам категорий Н4, Н5 и Н6 ввиду их исключительной роли в ИСГТ применяется комплекс особых организационных мер по их подбору, принятию на работ, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что лица категорий Н4, Н5 и Н6 относятся к доверенным лицам и поэтому исключаются из числа вероятных нарушителей.

Лица категории Н7 могут обладать информацией об алгоритмах и программах обработки информации на ИСПДн, возможностями внесения ошибок, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии разработки, внедрения и сопровождения, может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

Техническое обслуживание и поставка прикладного программного обеспечения производится исключительно доверенными организациями, поэтому лица категории Н7 исключаются из вероятных нарушителей.

Таким образом предполагается, что к вероятным нарушителям относятся лица категорий НІ, Н2 и Н8. Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

2.3. В качестве внешнего нарушителя информационной безопасности (категория НО) рассматривается нарушитель, который не имеет непосредственного доступа к аппаратным средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

К внешним нарушителям могут относиться:

- криминальные структуры;
- бывшие сотрудники - администраторы или пользователи ИСПДн;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке.

Предполагается, что содержание и объем персональных данных, находящихся в ИСПДн, не достаточны для мотивации разведывательных служб иностранных государств для реализации угроз безопасности ИСПДн.

Предполагаемые внешние нарушители знакомы с основными алгоритмами и протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также применяемыми принципами и концепциями безопасности. Предполагается, что они могут использовать стандартное и специальное оборудование для идентификации уязвимостей, либо для реализации угроз информационной безопасности. Данное оборудование может быть как частью штатных средств, так относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников). Предполагается, что лица категории НО относятся к вероятным нарушителям.

2.4. Предполагается, что нарушитель имеет следующие средства реализации угроз:

- аппаратные компоненты СЗПДн;
- доступные технические средства и программное обеспечение. Предполагается что содержание и объем персональных данных, находящихся в ИСПДн не достаточны для мотивации применения нарушителем специально разработанных технических средств и программного обеспечения. Внутренний нарушитель может использовать штатные средства. Для определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, имеющиеся в свободном доступе, или свободной продаже.

Раздел III

3. Описание объектов и целей реализации угроз информационной безопасности.

3.1. Основными информационными ресурсами, обрабатываемыми в ИСПДн являются следующие:

а) целевая информация:

- персональные данные и их резервные копии;

б) технологическая информация:

- защищаемая управляющая информация (конфигурационные файлы, таблиц маршрутизации, настройки системы защиты и пр.);
- защищаемая технологическая информация средств доступа к системам управления ИСПДн (аутентификационная информация и др.);
- информационные ресурсы ИСПДн на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами ИСПДн (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
- информация о СЗПДн, ее структуре, принципах и технических решениях защиты;
- информационные ресурсы ИСПДн (базы данных и файлы), содержащие информацию информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах.

в) программное обеспечение:

- ресурсы ИСПДн, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ИСПДн, программное обеспечение средств защиты.

3.2. Целью реализации угроз является нарушение определенных характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

Раздел IV

4. Описание каналов реализации угроз информационной безопасности.

4.1. Угрозы безопасности реализуются в результате образования канала реализации угроз, возникающего между источником угрозы и носителем ПДн, что создает необходимые условия возможного нарушения безопасности ПДн (несанкционированный или случайный доступ).

Возможными каналами реализации угроз УБПДн являются:

- каналы доступа, образованные с использованием программного обеспечения;
- каналы непосредственного доступа к объекту атаки (визуальный, физический);
- технические каналы утечки: каналы связи (как внутри, так и вне контролируемой зоны); каналы ПЭМИН (сигнальные цепи (информационные и управляющие интерфейсы СВТ), каналы передачи данных вычислительных сетей, источники и цепи электропитания, цепи заземления).

4.2. Таким образом, при обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

- угроз утечки акустической (речевой) информации;
- угроз утечки видовой информации;

– угроз утечки информации по ПЭМИН.

Раздел V

5. Исходный уровень защищенности ИСПДн.

5.1. Под исходным уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Yj). Для определения актуальности перечисленных угроз необходимо определить уровень исходной защищенности ИСПДн.

В соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России (далее - Методика), для нахождения уровня исходной защищенности ИСПДн, т.е. значения числового коэффициента Yj необходимо определить показатели исходной защищенности ИСПДн, которые представлены в таблице 2.

Таблица 2

№ п/п	Технические и эксплуатационные характеристики ИСПДн	Уровни защищенности		
		Высокий	Средний	Низкий
1.	По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2.	По наличию соединения с сетями общего пользования: ИСПДн, имеющая многоточечный выход в сеть общего пользования	-	+	-
3.	По встроенным (легальным) операциям с записями баз персональных данных: модификация, передача	-	-	+
4.	По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	-	+	-
5.	По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн, непринадлежащая организации-владельцу данной ИСПДН	-	-	+
6.	По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными	-	+	-
7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая часть ПДн	-	+	-

Из анализа результатов исходной защищенности следует, что уровню не ниже «средний» соответствуют не менее 70% характеристик ИСПДн.

Следовательно, в соответствии с Методикой ИСПДн имеет средний уровень исходной защищенности и числовой коэффициент Yi=5.

Раздел VI

6. Угрозы безопасности.

6.1. Согласно Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России в качестве базовой модели угроз безопасности ПДн при их обработке в ИСПДн следует принять «Типовую модель угроз безопасности персональных данных, обрабатываемых в локальных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена».

В соответствии с указанной типовой моделью угроз безопасности ПДн в ИСПДн рассматривают реализацию угроз утечки информации по техническим каналам и угроз НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

6.2. В соответствии со спецификой применяемых средств защиты, категорий ПДн, классификации нарушителей и рекомендациями базовой модели УБПДн далее рассмотрены следующие угрозы безопасности для ИСПДн:

- угрозы утечки видовой информации;
- угрозы утечки акустической информации;
- угрозы утечки информации по каналу ПЭМИН;
- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информация путем физического доступа к элементам ИСПДн;
- угрозы, реализуемые в ходе загрузки операционной системы;
- угрозы, реализуемые после загрузки операционной системы;
- угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрения ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение);
- угрозы «Анализ сетевого трафика» с перехватом передаваемой по сети информации;
- угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы «Отказ в обслуживании»;
- угрозы выявления паролей;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ;
- угрозы навязывания ложного маршрута сети.

Раздел VII

7. Основные способы реализации угроз информационной безопасности

7.1. При определении основных способов реализации угроз информационной безопасности ИСПДн учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла ИСПДн и ее компонентов, условий функционирования ИСПДн, а также предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности ИСПДн:

- несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн;
- негативные воздействия на программно-технические компоненты ИСПДн вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;
- методы социальной инженерии для получения сведений об ИСПДн для создания благоприятных условий применения других методов;

- использование оставленных без присмотра заблокированных средств администрирования ИСПДн;
- сбои и отказы программно-технических компонентов ИСПДн;
- внесение неисправностей, уничтожение аппаратных и программно-аппаратных компонентов ИСПДн путем непосредственного физического воздействия;
- осуществление несанкционированного доступа к информации при ее передаче.

Раздел VIII

8. Вероятность реализации УБПДн.

8.1. Под вероятностью реализации угрозы понимается определяемый методом экспертных оценок показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Оценка вероятности реализации УБПДн произведена методом экспертных оценок в соответствии с Методикой.

Числовой коэффициент (У2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

1. Маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2= 0).
2. Низкая вероятность -объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (У2 = 2).
3. Средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (У2= 5).
4. Высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты (У2= 10).

В соответствии с вышеуказанными определениями в таблице 3 приведена оценка вероятности (У2) реализации угроз безопасности для ИСПДн, а также обоснование значения У2 исходя из складывающихся условий обстановки, предпосылок для реализации угрозы и принятых мер по обеспечению безопасности ПДн в соответствии с анализом.

Таблица 3

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

По итогам оценки уровня исходной защищенности (Yi) и вероятности реализации угрозы (Y2) рассчитан коэффициент реализуемости угрозы (Y), и определена возможности реализации угрозы (таблица 3).

Коэффициент реализуемости угрозы рассчитывается по формуле:

Y= (Y1+Y2)/20.

Y=(5+5)/20=0,5 - возможность угрозы признается средней.

По значению коэффициента реализуемости угрозы Y формулируется вербальная интерпретация реализуемости угрозы следующим образом:

- если 0<Y<0,3, то возможность угрозы признается низкой;
- если 0,3<Y<0,6, то возможность угрозы признается средней;
- если 0.6<Y<0.8, то возможность угрозы признается высокой:

– если Y>0,8, то возможность угрозы признается очень высокой.

Раздел IX

9. Оценка опасности и актуальности УБПДн.

9.1. Оценка опасности угроз в ИСПДн произведена методом экспертных оценок по вербальному показателю опасности, который в соответствии с Методикой имеет три значения:

– низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
– средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
– высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Правила, по которым УБПДн были отнесены к актуальным, соответствуют требованиям Методики и приведены в таблице 3.

Оценка опасности и актуальности угроз в ИСПДн приведена в таблице 4.

Актуальные угрозы безопасности представлены в таблице 5.

Таблица 5

№ п/п	Наименование угрозы
1	Угрозы, реализуемые после загрузки ОС
2	Угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение)
3	Угрозы «Анализ сетевого трафика» с перехватом передаваемой по сети информации.
4	Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.
5	Угрозы подмены доверенного объекта
6	Угрозы типа «Отказ в обслуживании»
7	Угрозы выявления паролей
8	Угрозы удаленного запуска приложений
9	Угрозы навязывания ложного маршрута сети

Таблица 4. Оценка опасности и актуальности угроз ИСПДн

№ п/п	Нарушитель	Угрозы безопасности ИСПДн	Вероятность реализации угрозы Y2	Коэффициент реализации (У)	Возможность реализации	Оценка опасности	Актуальность угрозы
1.	**Угрозы утечки видовой информации**						
1.1.	Н0	Расположение ИСПДн делает маловероятным визуальный просмотр посторонними лицами информации на мониторе.	2				
1.2.	Н1, Н8	Неактуальна в связи с малой результативностью по сравнению с более действенными способами получения информации	0				
1.3.	Н2	Допущенные к обработке ПДн сотрудники ознакомлены под личную подпись с режимом конфиденциальности. принятым в ИСПДн.	0				
1.4.		Итого для угрозы:	2	0,35	средняя	низкая	Не актуальная
2.	**Угрозы утечки акустической информации**						
2.1.	НО	Акустические средства обработки отсутствуют	0				
2.2.	Н1,Н8	Акустические средства обработки отсутствуют	0				
2.3.	Н2	Акустические средства обработки отсутствуют	0				
2.4.		Итого для угрозы:	0	0,25	низкая	низкая	Не актуальная
3.	**Угрозы утечки по каналу ПЭМИН**						
3.1.	НО	Неактуальна в связи с малой результативностью по сравнению с более действенными способами получения информации	0				
3.2.	Н1.Н8	Неактуальна в связи с малой результативностью по сравнению с более действенными способами получения	0				

		информации					
3.3.	Н2	Неактуальна в связи с малой результативностью по сравнению с более действенными способами получения информации	0				
3.4.		Итого для угрозы:	0	0,25	низкая	низкая	Не актуальная
4.	**Угрозы хищения, разрушения (уничтожения), несанкционированного копирования носителей информации (встроенных или внешних накопителей, самих вычислительных средств, бумажных носителей, кража переносных хранилищ, воровство при выносе)**						
4.1.	НО	Маловероятна в связи с малой результативностью по сравнению с более действенными способами получения информации	2				
4.2.	Н1,Н8	Маловероятна в связи с малой результативностью по сравнению с более действенными способами получения информации	2				
4.3.	Н2	Допущенные к обработке ПДн сотрудники ознакомлены под личную подпись с режимом конфиденциальности, принятым в ИСПДн.	0				
4.4.		Итого для угрозы:	2	0,35	средняя	низкая	Не актуальная
5.	**Угрозы, реализуемые в ходе загрузки ОС**						
5.1.	НО	В здании введен контроль доступа в контролируемую зону. Доступ к загрузке ОС невозможен.	0				
5.2.	Н1,Н8	Администратором безопасности установлен пароль на BIOS, загрузка производится исключительно с жесткого диска.	0				
5.3.	Н2	Администратором безопасности установлен пароль на BIOS, загрузка производится исключительно с жесткого диска.	0				

5.4.		Итого для угрозы:	0		низкая	низкая	Не актуальная
6.	**Угрозы, реализуемые после загрузки ОС**						
6.1.	НО	В здании введен контроль доступа в контролируемую зону. Доступ к ИСПДн невозможен.	0				
6.2.	Н1.Н8	В отсутствии сотрудника допущенного к обработке ПДн компьютер автоматически блокируется	0				
6.3.	Н2	Высокая вероятность доступа к ПДн.	10				
6.4.		Итого для угрозы:	10	0,75	высокая	высокая	Актуальная
7.	Угрозы внедрения вредоносных программ (подмена ПО на программы с ВДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение)						
7.1.	НО	В здании введен контроль доступа в контролируемую зону. Доступ к ИСПДн невозможен. В организации установлены средства антивирусного контроля.	0				
7.2.	Н1,Н8	В организации установлены средства антивирусного контроля.	5				
7.3.	Н2	В организации установлены средства антивирусного контроля.	5				
7.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
8.	Угрозы «Анализ сетевого трафика» с перехватом передаваемой по сети информации.						
8.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ПДн.	5				
8.2.	Н1, Н8	Организационными мерами доступ внутри здания к сетевым ресурсам ИСПДн маловероятен.	5				
8.3.	Н2	Доступ к сетевым ресурсам с ограниченными правами.	2				
8.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не

							актуальная
9.	**Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.**						
9.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ПДн.	5				
9.2.	Н1, Н8	Организационными мерами доступ внутри здания к сетевым ресурсам затруднен.	5				
9.3.	Н2	Доступ к сетевым ресурсам с ограниченными правами.	2				
9.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
10.	**Угрозы подмены доверенного объекта**						
10.1.	НО	В связи с подключением к сетям общего пользования возможен удаленный доступ к ПДн, средняя вероятность.	5				
10.2.	Н1, Н8	Доступ возможен только с правами администратора, закрыт организационными мерами.	5				
10.3.	Н2	Доступ возможен только с правами администратора, закрыт организационными мерами.	2				
10.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
11.	**Угрозы типа «Отказ в обслуживании»**						
11.1.	НО	В связи с подключением к сетям общего пользования возможен удаленный доступ к ПДн, средняя вероятность.	5				
11.2.	Н1, Н8	Доступ возможен только с правами администратора, закрыт организационными мерами.	5				
11.3.	Н2	Доступ возможен только с правами администратора, закрыт организационными мерами.	2				

11.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
12.	**Угрозы выявления паролей**						
12.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ИСПДн, средняя вероятность.	5				
12.2.	Н1,Н8	Возможен просмотр паролей лицам, имеющими доступ в помещения. Средняя вероятность.	5				
12.3.	Н2	Использование сложных паролей. Блокировка при введении неверного пароля более трех раз. Подбор паролей невозможен.	2				
12.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
13.	**Угрозы удаленного запуска приложений**						
13.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ИСПДн, средняя вероятность.	5				
13.2.	Н1,Н8	Организационными мерами доступ внутри здания к сетевым ресурсам маловероятен.	5				
13.3.	Н2	Доступ возможен только с правами администратора, закрыт организационными мерами.	2				
13.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
14.	**Угрозы внедрения по сети вредоносных программ.**						
14.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ИСПДн, средняя вероятность.	5				
14.2.	Н1,Н8	Организационными мерами доступ внутри здания к сетевым ресурсам маловероятен.	5				
14.3.	Н2	Доступ возможен только с правами администратора, закрыт организационными мерами.	2				

14.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная
15.	**Угрозы навязывания ложного маршрута сети.**						
15.1.	НО	В связи с подключением к сетям общего пользования, возможен несанкционированный доступ к ИСПДн, средняя вероятность.	5				
15.2.	Н1,Н8	Организационными мерами доступ внутри здания к сетевым ресурсам маловероятен.	2				
15.3.	Н2	Доступ возможен только с правами администратора, закрыт организационными мерами.	2				
15.4.		Итого для угрозы:	5	0,5	средняя	низкая	Не актуальная

ЗАКЛЮЧЕНИЕ

ИСПДн является специальной информационной локальной, многопользовательской системой, с разграничением прав пользователей ИСПДн, имеющей подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Актуальные угрозы безопасности ПДн, установленные в ходе изучения ИСПДн представляют собой условия и факторы, создающие реальную опасность несанкционированного доступа к ПДн, с целью нарушения их конфиденциальности, целостности и доступности.

Угрозы утечки по техническим каналам, включающие в себя угрозы утечки акустической (речевой) информации, угрозы утечки видовой информации и угрозы утечки по каналу ПЭМИН в соответствии с уровнем исходной защищенности ИСПДн, условиями функционирования и технологиями обработки и хранения информации являются неактуальными.

В целях обоснованного подхода к обеспечению безопасности ПДн для нейтрализации актуальных угроз безопасности, выявленных согласно вышеизложенной модели угроз, в составе мероприятий по защите ПДн при их обработке в ИСПДн целесообразно использовать следующие методы:

- идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов;
- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);
- физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- межсетевое экранирование;
- использование средств антивирусной защиты.

К лицам категорий Н4, Н5 и Н6 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. В данную категорию должны включаться только доверенные лица.

Источники, использованные при разработке:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации информационных технологиях и о защите информации».