Министерство сельского хозяйства Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Новосибирский государственный аграрный университет»

УТВЕРЖДАЮ:

Ректор

_____ А.С. Денисов

«28» 04 2016 г.

Система менеджмента качества

МЕТОДИЧЕСКАЯ ИНСТРУКЦИЯ

Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных ФГБОУ ВО Новосибирский ГАУ

СМК МИ 21-01-2016

Экз. №___

ЛИСТ СОГЛАСОВАНИЙ

Разработал

Проректор по лицензированию, аккредитации и ИТ

_____ *Наумкин И.В.*

"27" 04 2016 г.

Директор ЦИТ

_____ *Каракулов А.В.*

"27" 04 2016 г.

Проверил

Начальник отдела менеджмента качества

_____ *Коршунова В.В.*

"27" 04 2016 г.

Начальник юридического отдела

_____ *Петровская Ю.С.*

"27" 04 2016 г.

Согласовано

Проректор по учебной работе

_____ *Бабин В.Н.*

"27" 04 2016 г.

1 Общие положения

1.1 Настоящая «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных ФГБОУ ВО Новосибирский ГАУ (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных (далее – УБПДн), при их обработке с использованием средств автоматизации.

Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, а также действиями зарубежных спецслужб или организаций (в том числе террористических), криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных (далее – ПДн), которые ведут к ущербу жизненно важным интересам личности, общества и государства.

1.2 Модель угроз содержит единые исходные данные по УБПДн, обрабатываемых в информационной системе (далее – ИС), связанными:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИС с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИС и обрабатываемых в ней ПДн с использованием программных и программно-аппаратных средств, с целью уничтожения или блокирования.

1.3 На основании Модели угроз решаются следующие задачи:

- анализ защищенности ИС от УБПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего уровня защищенности ПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа (далее – НСД) к обрабатываемым ПДн и (или) передачи их лицам, не имеющим права доступа к ним;
- недопущение воздействия на технические средства ИС, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности ПДн, обрабатываемых в ИС.

2 Перечень условных обозначений и сокращений

АРМ	автоматизированное рабочее место
БД	база данных
ИБ	информационная безопасность
ИС	информационная система
ИСПДн	информационная система персональных данных
КЗ	контролируемая зона
ЛВС	локальная вычислительная сеть
НСД	несанкционированный доступ
ОИ	объект информатизации
ОРД	Организационно-распорядительная документация
ОС	операционная система
ПДн	персональные данные

ПЗУ	постоянное запоминающее устройство
ПО	программное обеспечение
ППЗУ	программируемое постоянное запоминающее устройство
ПРД	правила разграничения доступа
ПЭМИН	побочные электромагнитные излучения и наводки
РФ	Российская Федерация
СВТ	средства вычислительной техники
СЗИ	средство защиты информации
СКЗИ	средство криптографической защиты информации
СУБД	система управления базами данных
СФ	среда функционирования СКЗИ
СФК	среда функционирования криптосредств
ТЗИ	техническая защита информации
ТКУИ	технический канал утечки информации
ТС	технические средства
УБПДн	угрозы безопасности персональных данных
УЗ ПДн	уровень защищенности персональных данных
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

3 Термины и определения

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

Автоматизированное рабочее место (АРМ) – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

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.

Доступ в операционную среду компьютера (информационной системы) – 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 (ИТ) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

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

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

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Канал связи – совокупность технических устройств, обеспечивающих передачу сообщений любого вида от отправителя к получателю, осуществляемую с помощью электрических сигналов.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также 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.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

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

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз.

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.

Недокументированные (недекларированные) возможности (НДВ) – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации.

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

Носитель информации – 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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Объект информатизации (ОИ) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

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.

Основные технические средства и системы (ОТСС) – ТС и системы, а так же их коммуникации, используемые для обработки, хранения и передачи информации, составляющей государственную тайну и иной информации конфиденциального характера.

Отказ в обслуживании – препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы.

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

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки (ПЭМИН) – 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.

Потенциал нарушителя – мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

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

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

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.

Программно-аппаратная закладка – совокупность технических и программных средств, которые могут осуществлять программно-математические воздействия.

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 (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средства криптографической защиты информации (СКЗИ, криптосредства) – шифровальные (криптографические) средства, предназначенные для защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Среда функционирования криптосредства (СФ) – совокупность технических и программных средств, совместно с которыми штатно функционирует криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

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

Узел сети – компьютер, терминал или другое устройство, подключенное к сети и имеющее уникальный адрес, позволяющий другим узлам сети связываться с ним по каналам связи.

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

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

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.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

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

Шифровальные (криптографические) средства (средства криптографической защиты информации, СКЗИ, криптосредства):

- ***средства шифрования*** – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

- ***средства имитозащиты*** – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

- ***средства электронной подписи***;

- ***средства кодирования*** – средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

- ***средства изготовления ключевых документов*** – аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России от 14.02.2008);

- Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах»;

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России от 21.02.2008 № 149/54-144);

- ГОСТ 15971-90 «Системы обработки информации. Термины и определения»;

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения»;

- ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

5 Общие сведения

5.1 Описание ИСПДн

Информационная система персональных данных (далее - ИСПДн или ИСПДн «НГАУ») предназначена для сбора, уточнения, использования, передачи ПДн субъектов ПДн, подавших заявление на обучение в ФГБОУ ВО Новосибирский ГАУ.

ИСПДн обеспечивает взаимодействие с Федеральной информационной системой обеспечения проведения государственной итоговой аттестации (далее – ФИС ГИА и приема) и Федеральной информационной системой «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (далее – ФИС ФРДО).

Создание ИСПДн осуществлялось в соответствии с реализацией:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- Постановление Правительства Российской Федерации от 27.01.2012 № 36 «Об утверждении Правил формирования и ведения федеральной информационной системы обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего профессионального образования и региональных информационных систем обеспечения проведения единого государственного экзамена»;

- Письмо Рособрнадзора от 12.04.2012 № 08-22 «О внесении сведений в федеральную информационную систему обеспечения проведения единого государственного экзамена и приема граждан в ССУЗы и ВУЗы»;

- Правил приема на обучение по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в «Новосибирский государственный аграрный университет» на 2016/17 учебный год.

ИСПДн обеспечивает хранение, обработку и другие операции, необходимые для устойчивого, непрерывного функционирования и бесперебойной работы ФГБОУ ВО Новосибирский ГАУ.

Состав ПДн, обрабатываемых в ИСПДн, и срок их хранения представлены в таблице 1.

Таблица 1. Состав персональных данных

Вид информации	Состав сведений	Операции	Срок хранения
Персональные данные абитуриентов и обучающихся	1. фамилия, имя, отчество; 2. адрес по прописке; 3. документ, удостоверяющий личность: a. серия; b. номер; c. кем и когда выдан; 4. дата рождения; 5. гражданство; 6. фамилии, имена, отчества родителей; 7. телефонный номер; 8. информация об образовании: a. наименование образовательного учреждения; b. сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность; 9. информация о трудовом стаже; 10. информация о знании иностранных языков	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, удаление, уничтожение.	10 лет, до отзыва субъектом своих ПДн

5.2 Защищаемые ресурсы

ИСПДн ФГБОУ ВО Новосибирский ГАУ представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными охраняемыми элементами (защищаемыми ресурсами) ИСПДн являются:

– ПДн, содержащиеся в ИС, согласно таблице 1;

– КТС, осуществляющие обработку ПДн (СВТ, компоненты ЛВС, средства и системы передачи, приема и обработки ПДн): 1 АРМ, сетевой коммутатор, маршрутизатор;

– Программные средства. ОС: Microsoft Windows 7 Professional Service Pack 1 (Microsoft), ПО: пакет офисных программ Microsoft Office Professional 10 (Microsoft), браузер Mozilla Firefox (Mozilla Corporation), текстовый редактор Notepad++ (Notepad++ Contributors), файловый менеджер Far Manager 3.0 (Евгений Рошал, FAR Group);

– ВТСС, их коммуникации, не предназначенные для обработки ПДн, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, но размещенные в помещениях, в которых расположены ТС ИСПДн, такие как СВТ, средства и системы кондиционирования, средства электронной оргтехники и т.п.

ИСПДн подключена к информационно-телекоммуникационной сети Интернет. Используется источник бесперебойного питания. В ИСПДн не используются съемные носители для обработки ПДн.

Для защиты ИСПДн «НГАУ» применяются следующие СЗИ:

- средство АВЗ: Kaspersky Endpoint Security 10 для Windows (сертификат соответствия ФСТЭК России №3025);

- средство анализа защищенности «Сетевой сканер безопасности XSpider 7.8.24» (сертификат соответствия ФСТЭК России № 3247);

- СКЗИ и МЭ: ПК ViPNet Client 3.2 (сертификаты соответствия: ФСБ России № СФ/525-2224, № СФ/124-2178, № СФ/124-2796, ФСТЭК России № 1549/1);

- СЗИ от НСД Dallas Lock 7.7 (сертификат соответствия ФСТЭК России № 2209).

В ИСПДн «НГАУ» отсутствуют средства для защиты от электромагнитных воздействий и от утечки по техническим каналам. Используются программные и технические средства, не содержащие НДВ в системном и прикладном ПО, нарушающие требования по обеспечению безопасности.

5.3 Технология обработки

ИСПДн «НГАУ» предназначена для работы в рабочие дни с 9:00 до 18:00. Возможны остановы компонент системы для проведения регламентных работ по техническому обслуживанию. Обработка ПДн осуществляется с помощью программных средств для автоматизации технологических процессов. Технология обработки ПДн предусматривает хранение информации на АРМ. Резервное копирование данных не осуществляется.

Заявления с ПДн и сведения о документах об образовании и о квалификации, документах об обучении на бумажных носителях хранятся в личном деле в отделе по учету студентов. Оператор – пользователь ИСПДн «НГАУ», вручную обрабатывает данные и через web-интерфейс загружает и отправляет на порталы ФИС ГИА и ФИС ФРДО.

Для организации защищенного взаимодействия в ИСПДн применяется ViPNet Client 3.2 -программный комплекс, выполняющий на рабочем месте пользователя с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

Обсуждение ПДн, раскрывающее признаки, идентифицирующие субъектов ПДн, не осуществляется. Звуковое воспроизведение ПДн не производится.

5.4 Правила доступа к защищаемой информации и техническим средствам ИСПДн «НГАУ»

ИСПДн «НГАУ» расположена в здания по адресу: г. Новосибирск, ул. Добролюбова, 160.

Вход в здание главного корпуса по адресу 630039, ул. Добролюбова, 160 осуществляется через главный вход с пропускным режимом и контролируется круглосуточно службой охраны. Служебные входы главного корпуса, а так же территории с условным обозначением «ВСТАВКА» закрыты на ключ или электронный замок с магнитным ключом. Ключ от служебных выходов хранится у ответственных сотрудников ВУЗа и на вахте.

Доступ в помещение посторонних лиц ограничен и осуществляется только в присутствии уполномоченных сотрудников ФГБОУ ВО Новосибирский ГАУ. Кабинет закрываются на ключ, сдается на вахту и хранится в сейфе.

За администрирование ИСПДн «НГАУ» ответственны сотрудники Центра информационных технологий ФГБОУ ВО Новосибирский ГАУ (далее – ЦИТ).

Регистрация пользователей, не являющихся работниками оператора, так же удаленный доступ к АРМ не предусмотрены.

В силу специфики среды функционирования ИСПДн пользователи имеют разные полномочия на доступ к информационным, программным и аппаратным ресурсам ИСПДн.

5.5 Анализ режимных и организационных мер по обеспечению информационной безопасности

Охрана контролируемой зоны ФГБОУ ВО Новосибирский ГАУ осуществляется в круглосуточном режиме, по договору об оказании охранных услуг № ДП-2015/52 от 26.06.2015.

Рабочая станция оснащена источником бесперебойного питания. Помещения ФГБОУ ВО Новосибирский ГАУ оборудованы пожарной сигнализацией. Коридоры, фойе и периметр здания оснащены системой видеонаблюдения.

Для ИСПДн отсутствует полный комплект ОРД по обеспечению ИБ.

В качестве общего ПО ИСПДн используется лицензионное ПО с действующей технической поддержкой от фирм-производителей или ПО свободного распространения с открытым исходным кодом.

Доступ к ИСПДн реализован на основе принятых ролевых моделей, принципов разделения обязанностей и минимизации полномочий с использованием средств аутентификации и авторизации.

5.6 Характеристики ИСПДн «НГАУ»

В соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства РФ от 01.11.2012 № 1119), ИСПДн «НГАУ» обладает характеристиками, приведенными в таблице 2.

Тип УБПДн, актуальных для ИСПДн «НГАУ», определяется с учетом оценки возможного вреда. Недокументированные (недекларированные) возможности могут присутствовать в системном или прикладном ПО.

В ИСПДн на системном уровне используются типовые продукты, программные компоненты которых получены в готовом виде (без конструкторской документации, без исходных текстов). На прикладном уровне используются продукты, программные компоненты которых получены как в готовом виде (без конструкторской документации, без исходных текстов), так и открытое ПО.

Таблица 2. Характеристики ИСПДн

Название ИСПДн	Категория ПДн	Тип субъектов ПДн	Объем одновременно обрабатываемых ПДн	Тип угроз
ИСПДн «НГАУ»	Иные категории ПДн	Персональные данные субъектов ПДн, не являющихся сотрудниками оператора	Данные менее, чем 100 000 субъектов ПДн	Угрозы 3-го типа

Предполагается, что уровень компетенции потенциальных нарушителей является недостаточным для использования НДВ системного и прикладного ПО.

Предполагается, что разработчики ПО не внедряют преднамеренно НДВ в разрабатываемые программы, так как для обеспечения безопасного и надежного функционирования ПО используются программные и технические средства проверенных и надежных производителей, поставщиков и разработчиков. Нарушение требований по обеспечению безопасности влечет финансовые и репутационные риски для производителей/поставщиков/ разработчиков и может послужить основанием для расторжения контрактов (заключенных договоров). Таким образом, производители, поставщики и разработчик ПО заинтересованы в соблюдении указанных требований своими сотрудниками.

В ИСПДн к открытому ПО предоставляется доступ только сотрудникам ЦИТ. Предполагается, что сотрудники ЦИТ относятся к доверенным лицам и исключаются из числа потенциальных лиц. Таким образом, исключается преднамеренное внедрение НДВ в открытое ПО.

Вероятность реализации угроз 1 и 2 типа безопасности в ИСПДн, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, признана маловероятной в связи с тем, что отсутствуют объективные предпосылки для реализации данных угроз.

С учетом вышеизложенного для ИСПДн признаются актуальными угрозы 3-его типа, т.е. не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО.

В результате определения уровня защищенности персональных данных для ИСПДн «НГАУ» определен 4 (четвертый) УЗ ПДн.

Вывод:

Для ИСПДн «НГАУ» определен 4 (четвертый) уровень защищенности ПДн (УЗ4). Структурная схема ИСПДн «НГАУ» представлена на рис. 1.

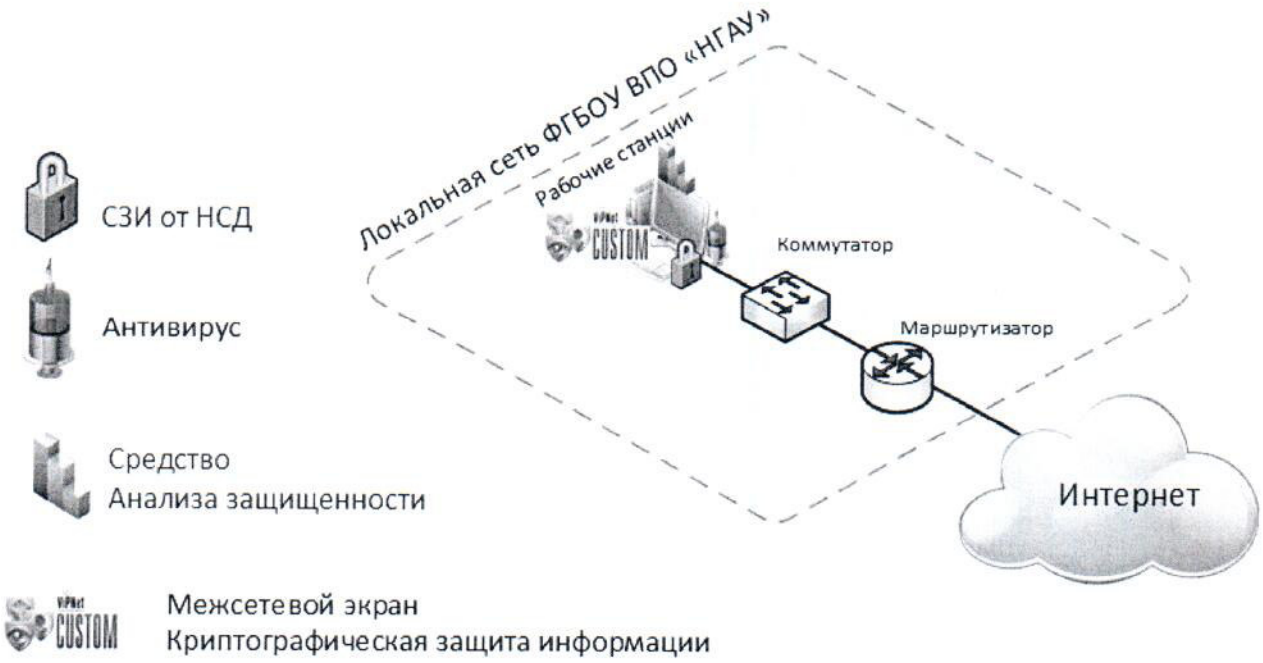

Рис. 1. Схема ИСПДн «НГАУ»

6 Возможные угрозы несанкционированного доступа к информации

6.1 Источники угроз несанкционированного доступа

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель (п. 4.1.1 Модели угроз);

- аппаратная закладка (п. 4.1.2 Модели угроз);
- носитель вредоносной программы (п. 4.1.3 Модели угроз).

Возможности источников УБПДн обусловлены наличием методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

6.1.1 Модель нарушителя безопасности персональных данных

Первичным источником угроз является нарушитель безопасности. Под нарушителем безопасности (далее – нарушитель) понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение характеристик безопасности защищаемых информационных ресурсов.

6.1.1.1 Описание нарушителя

С точки зрения наличия права легального постоянного или разового доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на две категории:

- категория I – лица, не имеющие права доступа в КЗ ИСПДн;
- категория II – лица, имеющие право постоянного или разового доступа в КЗ ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов КЗ;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах КЗ.

Лица, имеющие право доступа в КЗ ИСПДн, также могут осуществлять атаки из-за пределов КЗ, поэтому констатируется, что:

- к внешним нарушителям можно отнести как лиц категории I, так и лиц категории II;
- к внутренним нарушителям можно отнести только лиц категории II.

1) Внешние нарушители (категория И0) – лица, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Внешний нарушитель имеет следующие возможности:

- осуществлять НСД к каналам связи, выходящим за пределы служебных помещений;
- осуществлять НСД через АРМ, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять НСД к защищаемой информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять НСД через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ;
- осуществлять НСД через ИС взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

2) Внутренние нарушители – лица, имеющие право доступа к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к защищаемой информации и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к защищаемой информации.

Первая категория (И1) – лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к защищаемой информации.

Лицо этой категории может:

- иметь доступ к фрагментам информации, содержащей защищаемую информацию и распространяющейся по внутренним каналам связи ИСПДн;

- обладает полной информацией об ИСПДн;
- обеспечивать функционирование и поддержку работоспособности СЗИ;
- проводить инструктаж эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ;
- осуществлять мониторинг и аудит ИБ;
- осуществлять контроль и предотвращение несанкционированного изменения целостности ресурсов;
- осуществлять контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения.

Седьмая категория (И7) – программисты-разработчики, поставщики прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории может:

- обладать наличием информации об алгоритмах и программах обработки информации в ИСПДн;
- обладать возможностями внесение ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии ее разработки, внедрения и сопровождения;
- располагать любые фрагменты информации о топологии ИСПДн и ТС обработки и защиты ПДн, обрабатываемых в ИСПДн.

Восьмая категория (И8) – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт ТС в ИСПДн.

Лицо этой категории может:

- осуществлять внесение закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- знать любые фрагменты информации о топологии ИСПДн и ТС обработки и защиты информации в ИСПДн.

Данная классификация нарушителей построена по иерархическому принципу, т.е. возможности нарушителя более высокого типа или категории Иi+1 включают в себя возможности нарушителей предыдущих типов и категорий Иi ($1 \le i \le 6$).

На основании «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России от 21.02.2008 № 149/54-144) различают шесть основных типов нарушителей:

- внешние нарушители типа Н1;
- административный персонал (охрана, работники инженерно-технических служб и т.д.) ИС типа Н2;
- пользователи ИС типа Н3;
- привилегированные пользователи ИС, осуществляющие непосредственный доступ к ТС (системные администраторы, администраторы безопасности, технические специалисты, осуществляющие функции физической (в т.ч. периметровой) защиты и обеспечивающие поддержание установленных режимов безопасности.) типа Н4;
- программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение в ИС, не являющиеся пользователями ИС, но имеющие право доступа (временного или постоянного) в КЗ, относятся к типу Н5;
- спецслужбы и представители специальных органов (контролирующих, правоохранительных, надзорных и т.п.) имеющих возможность применять специальные средства и способы атак, а также специализирующиеся в области анализа СКЗИ и СФК, относятся к типу Н6.

Вывод:

К внешним нарушителям И0 ИСПДн «НГАУ» могут быть отнесены представители преступных организаций, бывшие работники, посторонние лица, пытающиеся получить доступ к защищаемой информации в инициативном порядке (физические лица).

К внутренним потенциальным нарушителям И1 можно отнести административный персонал, проводящий работы в помещениях, в которых размещаются ТС ИСПДн «НГАУ», а так же работников, осуществляющих функции физической (в т.ч. периметровой) работы: энергетики, сантехники, уборщицы, работники охраны и другие лица, обеспечивающие нормальное функционирование ОИ и обеспечивающие поддержание установленных режимов безопасности ИСПДн «НГАУ».

К внутренним потенциальным нарушителям И2 в ИСПДн «НГАУ» можно отнести работников ФГБОУ ВО Новосибирский ГАУ зарегистрированных пользователей ИСПДн «НГАУ» в основном, которые занимаются обработкой защищаемой информации в КЗ.

Внутренний нарушитель И3 отсутствует, поскольку в ФГБОУ ВО Новосибирский ГАУ не используется удаленный доступ, к защищаемым ресурсам ИСПДн по локальным и (или) распределенным ИС.

К внутренним потенциальным нарушителям И4 в ИСПДн «НГАУ» можно отнести работников ФГБОУ ВО Новосибирский ГАУ, отвечающих за криптографическую защиту информации и за эксплуатацию СКЗИ, которые в свою очередь выполняют правила, оговоренные в инструкции ответственного пользователя за эксплуатацию СКЗИ (администратора СКЗИ) и осуществляют:

- конфигурирование и административную настройку СКЗИ;
- поэкземплярный учет используемых оператором криптосредств, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ;
- учет пользователей криптосредств;
- хранение эксплуатационной и технической документации к криптосредствам, ключевым документам, носителям дистрибутивов криптосредств, бумажных и машинных носителей защищаемой информации;
- расследования и составление заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности персональных данных;
- разработку и принятие мер по предотвращению возможных негативных последствий нарушений.

К внутренним потенциальным нарушителям И5 в ИСПДн «НГАУ» можно отнести работников с правами администратора ИСПДн, выполняющих правила, оговоренные в инструкции администратора ИСПДн (конфигурирование и управление ПО и оборудованием).

К внутренним потенциальным нарушителям И6 в ИСПДн «НГАУ» можно отнести администратора ИБ, выполняющего правила, оговоренные в инструкции администратора ИБ, отвечающего за соблюдение ПРД, за генерацию ключевых элементов, смену паролей.

К внутренним потенциальным нарушителям И7 в ИСПДн «НГАУ» можно отнести программистов-разработчиков, поставщиков и лиц осуществляющих техническое сопровождение ПО (в том числе СЗИ и СКЗИ), не являющихся санкционированными пользователями ИСПДн, но имеющих разовый доступ в КЗ. Так же к И7 можно отнести работников сторонних организаций, осуществляющих услуги по договорам и входящих в службу технической поддержки.

К внутренним потенциальным нарушителям И8 в ИСПДн «НГАУ» можно отнести работников ФГБОУ ВО Новосибирский ГАУ, а также работников сторонних организаций, не являющихся санкционированными пользователями ИСПДн, но имеющих разовый доступ в КЗ, и осуществляющих поставку, сопровождение и ремонт ТС.

На основании вышеизложенного и исходя из возможностей, каждому типу нарушителей произведено отнесение категорий потенциальных нарушителей:

- Лиц категории И1 можно отнести к типу нарушителей Н2;
- Лиц категории И2 можно отнести к типу нарушителей Н3;
- Лиц категории И3 можно отнести к типу нарушителей Н3;
- Лиц категории И4 можно отнести к типу нарушителей Н4;
- Лиц категории И5 можно отнести к типу нарушителей Н4;
- Лиц категории И6 можно отнести к типу нарушителей Н4;
- Лиц категории И7 можно отнести к типу нарушителей Н5;
- Лиц категории И8 можно отнести к типу нарушителей Н2.

6.1.1.2 Модель нарушителя для этапа разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных СКЗИ и среды функционирования

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных СКЗИ и СФ обработка защищаемой информации не производится. Поэтому объектами атак могут быть только сами эти средства и документация на них.

Соответствие технических и программных средств СКЗИ, СФ и документации на эти средства, поступающих в зону ответственности ФГБОУ ВО Новосибирский ГАУ, эталонным образцам подтверждается предоставлением гарантии производителя (поставщика) ТС, а так же гарантийным письмом производителя (поставщика) ТС о соответствии технических и программных СКЗИ, СФ и документации на эти средства.

Контроль целостности технических и программных средств СКЗИ и СФ и документации на эти средства в процессе хранения и ввода в эксплуатацию этих средств осуществляется ФГБОУ ВО Новосибирский ГАУ с использованием как механизмов контроля, описанных в документации, на СКЗИ, так и с использованием организационных и организационно-технических мер, разработанных с учетом требований соответствующих нормативных и методических документов.

6.1.1.3 Модель нарушителя для этапа эксплуатации технических и программных СКЗИ и среды функционирования

На этапе эксплуатации технических и программных СКЗИ и СФ определяются цели и возможные объекты атак.

Возможными объектами атак в ИСПДн являются:

- документация на СКЗИ и на технические и программные компоненты СФ;
- защищаемая информация;
- ключевая, аутентифицирующая и парольная информация;
- СКЗИ (программные и аппаратные компоненты СКЗИ);
- технические и программные компоненты СФ;
- данные, передаваемые по каналам связи;
- помещения, в которых находятся защищаемые ресурсы ИС.

Возможными направлениями несанкционированных действий нарушителя являются:

- доступ к защищаемой информации с целью нарушения ее конфиденциальности (хищения, ознакомления, перехват);
- доступ к защищаемой информации с целью нарушения ее целостности (модификации данных);
- доступ к техническим и/или программным средствам с целью постоянного (уничтожения) или временного нарушения доступности защищаемой информации для пользователей;
- доступ к техническим и программным средствам с целью внесения в них несанкционированных изменений, создающих условия для проведения атак;
- доступ к СЗИ с целью изменения их конфигурации или блокирования работы.

6.1.1.4 Определение потенциальных нарушителей

Предполагается, что все потенциальные нарушители самостоятельно проводят подготовку и разработку методов и средств, необходимых для проведения атак на элементы ИСПДн.

Рассматриваются угрозы, связанные с действиями внешних нарушителей И1. К внешним нарушителям (посторонним лицам) типа Н1 в ИСПДн можно отнести любых лиц, которые не имеют непосредственного доступа к ТС и ресурсам ИСПДн, находящимся в пределах КЗ.

Предполагается, что объем и состав обрабатываемых и хранимой в ИСПДн информации является недостаточным для возможной мотивации внешних нарушителей к осуществлению действий, направленных на утечку информации по каналам ПЭМИН. Кроме того, обработка части информации, содержащейся в ИСПДн, при выводе ее на экраны мониторов и другие периферийные устройства занимает минимальный отрезок времени, в связи с чем риск утечки по каналам ПЭМИН является пренебрежимо малым. Так же в помещении ИСПДн отсутствуют окна.

Исходя из особенностей функционирования ИСПДн, допущенные к ней работники имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн.

При получении доступа к ИСПДн лица категории И2 в обязательном порядке изучают инструкции, регламентирующие порядок работ и требования по обеспечению безопасности ПДн и подписывают соглашение о конфиденциальности, либо ознакамливаются с положениями регламентов, определяющих порядок обработки и защиты ПДн. Далее пользователи ИСПДн «НГАУ» проходят инструктаж по работе в ИСПДн и предупреждаются об ответственности за нарушение правил работы. Таким образом, лица, отнесенные к типу Н3, исключаются из числа потенциальных нарушителей.

Привилегированные пользователи ИСПДн «НГАУ» (лица, отнесенные к категориям И4–И6), осуществляющие техническое обслуживание аппаратных и программных средств ИСПДн и СЗИ, включая их настройку, конфигурирование и предоставление доступа другим пользователям, назначаются из числа доверенных лиц. Эффективность всей системы безопасности ПДн зависит от адекватности действий данных лиц. Указанные лица принимаются на работу на основе специальных кадровых и организационно-штатных мероприятий, гарантирующих их квалификацию, лояльность и ответственность (в договорах и должностных инструкциях работников определяются их обязанности и ответственность в случае нарушения требований ИБ), подписывают соглашение о конфиденциальности. Поэтому устанавливать систему защиты от них было бы нецелесообразным в связи с её беспрецедентной сложностью и низкой эффективностью (исходя из соображений, что если кто-то из этих лиц преднамеренно задумает нарушить безопасность защищаемой информации, то предупредить реализацию такой угрозы можно только в комплексе со специальными мероприятиями оперативного обеспечения, режима и контроля, сложность которых несоразмерна с более простыми возможностями привилегированных лиц, обойти установленные для них ограничения). Вместе с тем, необходимо учитывать, что контроль за деятельностью привилегированных пользователей и оценка их эффективности осуществляется в ходе оценки соответствия ИСПДн по требованиям безопасности при проведении аттестации и проверок со стороны регулирующих органов (ФСБ России, ФСТЭК России), а также со стороны правоохранительных органов. Следовательно, привилегированные пользователи ИСПДн «НГАУ» типа Н4 исключаются из числа потенциальных внутренних нарушителей.

Лица И1 и И8 являются внутренними сотрудниками, а также сотрудниками сторонних организаций, осуществляющими работу в соответствии с контрактами (заключенными договорами). В рамках выполнения своих должностных обязанностей данные лица могут иметь физический доступ к ТС ИС, к носителям информации, но не могут иметь доступа к информационным и программным ресурсам ИСПДн. В связи с этим и, в соответствии с установленным режимом обеспечения безопасности, обслуживание помещений, в которых расположены компоненты ИС, производится в присутствии штатных сотрудников-

пользователей ИСПДн. Таким образом, лица, отнесенные к типу Н2, исключаются из числа потенциальных нарушителей.

Лица И7 представляют доверенные организации в соответствии с обоснованиями, описанными в п.2.6 настоящей Модели угроз. Перед заключением договора (контракта) на разработку и поставку ПО проводится ряд организационно-штатных мероприятий, обеспечивающий выбор организаций, заслуживающих доверие. Лица, обеспечивающие сопровождение ПО в ИСПДн, имеют доступ в КЗ только в присутствии и под контролем привилегированных пользователей. Таким образом, лица категории Н5 исключаются из числа потенциальных внутренних нарушителей.

К типу нарушителей Н6 можно отнести служащих органов исполнительной власти и подведомственных им структур, осуществляющих проверку ИСПДн, либо совершающих иные действия в соответствии с нормативно-правовыми актами РФ, например организации, являющиеся лицензиатами ФСТЭК России и ФСБ России. В связи с чем, предполагается, что лица, отнесенные к типу Н6, считаются доверенными и исключаются из числа потенциальных нарушителей.

Различают высокий, средний и низкий потенциалы нарушителя:

- Высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.
- Средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей.
- Низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Вывод:

Лица, отнесенные к типу Н3, Н4, в соответствии с приведенным описанием располагают наибольшей информацией об ИСПДн и возможностями для совершения атак. Предполагается, что возможность сговора этих лиц с внешними нарушителями маловероятна, в виду того, что эти лица считаются доверенными и исключаются из числа потенциальных нарушителей.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков ИСПДн, а также сговора внутреннего и внешнего нарушителей исключена применением организационно-технических и кадрово-режимных мер, действующих на объекте размещения ИСПДн.

Возможный сговор внешних нарушителей не дает никаких дополнительных преимуществ по сравнению с индивидуальным внешним нарушителем.

Предполагается, что потенциальные нарушители являются одиночными нарушителями, самостоятельно осуществляющими освоение способов, подготовку и проведение атак и не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ

Иностранные разведки и организованные преступные группировки (включая сговор с ними), в качестве нарушителей, не рассматриваются исходя из предположения, что для них, по своим потенциальным возможностям, проведение атак является средством менее предпочтительным, чем средства, основанные на агентурных методах, которые они предпринимают в целях получения конкретно интересующей их информации, или информации о конкретно интересующем их лице, а не по всей БД в ИСПДн.

Таким образом, на основании вышеизложенного, предполагается, что к потенциальным нарушителям в ИСПДн «НГАУ» относятся лица типа Н1 (категория И0) с низким потенциалом.

6.1.1.5 Предложение об имеющейся у нарушителя информации об объектах атак

Предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации атак, за исключением информации, доступ к которой со стороны

нарушителя исключается СЗПДн в зоне ответственности оператора ИСПДн. Соответственно при имеющихся ограничениях (системы защиты) в ИСПДн, устанавливается нижеперечисленное:

- Потенциальному нарушителю не известна ключевая, парольная и другая аутентифицирующая информация, доступ к которой исключается функционирующей СЗПДн.

- Потенциальному нарушителю доступна только документация на СКЗИ и СФ, имеющаяся в свободной продаже. Потенциальному нарушителю не известны исходные тексты прикладного ПО, в зоне ответственности заказчика и оператора исходные тексты прикладного ПО криптосредств отсутствуют.

- Потенциальному нарушителю не известны долговременные ключи СКЗИ: организационно-режимными мерами долговременные ключи криптосредства хранятся на физически защищенных носителях, доступ к которым имеют только доверенные лица, прошедшие инструктаж. Производится регулярная смена ключей в соответствии с требованиями к данным продуктам.

- Потенциальному нарушителю не могут быть известны данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.д.), в соответствии с организационно-режимными мерами, а также неактуальностью угроз утечки ПДн по каналам ПЭМИН.

- Потенциальному нарушителю не могут быть известны сведения о линиях связи, по которым передаются ПДн, так как маршрут передачи данных и структура линий связи определяется провайдером, данная информация является конфиденциальной, и провайдер не имеет права предоставлять кому-либо данную информацию.

- Потенциальному нарушителю не известны все сети связи, работающие на едином ключе: в ИС используются СКЗИ, имеющие индивидуальные ключи (нет сетей связи, работающих на едином ключе).

- Потенциальному нарушителю, так как в ИСПДн используются сертифицированные СКЗИ, не могут быть известны все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации СКЗИ и СФ, а так же неисправности и сбои ТС СКЗИ и СФ.

- Потенциальному нарушителю, в соответствии с организационно-режимными мерами, а также неактуальностью угроз утечки ПДн по каналам ПЭМИН, не представляется возможность перехвата сигналов от ТС СКЗИ и СФ.

6.1.1.6 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что вероятные нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и ПО, в том числе программные и аппаратные компоненты криптосредств;

- специально разработанные ТС и ПО;

- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Дополнительные возможности по получению аппаратных компонент СКЗИ и СФ у нарушителей отсутствуют, ввиду того, что организационно-режимными мерами невозможен неконтролируемый доступ в помещения, в которых расположены аппаратные компоненты СКЗИ и СФ.

Предполагается, что объем и состав обрабатываемых и хранимых в ИСПДн ПДн является недостаточным для возможной мотивации нарушителей к созданию средств атак в научно-исследовательских центрах.

Возможности по получению доступа к штатным средствам у нарушителей отсутствуют, ввиду того, что потенциальным нарушителем невозможен неконтролируемый доступ в помещения, в которых расположены штатные средства ИСПДн.

6.1.1.7 Описание каналов атак

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

Основными каналами угроз являются каналы связи (как внутри, так и вне КЗ), не защищенные от НСД к информации в соответствии с нормативно-правовыми актами РФ, а также штатные средства.

Возможными каналами угроз, в частности, рассматриваются:

- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
- машинные носители информации;
- носители информации, выведенные из употребления;
- ТКУИ;
- сигнальные цепи;
- цепи электропитания;
- цепи заземления;
- канал утечки за счет электронных устройств негласного получения информации;
- информационные и управляющие интерфейсы СВТ.

Предполагается, что в число возможных каналов атак не входят каналы утечки за счет ПЭМИН, в связи с тем, что объем и состав обрабатываемых и хранимых в ИС ПДн является недостаточным для возможной мотивации внешних нарушителей к осуществлению действий, направленных на утечку ПДн по каналам ПЭМИН.

В силу действующих правил доступа и должностных обязанностей существуют ограничения на доступ потенциальных нарушителей к каналам атак.

Возможности по получению доступа к каналам непосредственного доступа к объекту атаки (акустический, визуальный, физический) у нарушителей отсутствуют, ввиду принятых мер по обеспечению физической безопасности.

В соответствии с принятыми для ИСПДн организационно-режимными мерами внешние нарушители не имеют доступа в помещения, в которых расположены ТС ИСПДн в отсутствии лиц, работающих в этих помещениях, и, соответственно, не могут получить доступ к машинным носителям информации.

Исключается получение информации с носителей, выведенных из употребления, т.к. ПДн, подлежат уничтожению без возможности восстановления путем физического уничтожения носителя, либо затирания ПДн.

В соответствии с принятыми для ИСПДн организационно-режимными мерами нарушители не имеют права доступа к информационным и управляющим интерфейсам СВТ, входящих в состав ИСПДн.

6.1.1.8 Тип нарушителя при использовании в информационной системе криптографических средств защиты информации

При взаимодействии и обмене информацией между ИСПДн и внешними по отношению к оператору ИС по сетям связи общего пользования и (или) сетям международного информационного обмена, а также при передаче защищаемой информации по кабельным системам, расположенным в пределах КЗ и не защищенных от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности защищаемой информации необходимо использование СКЗИ.

Уровень криптографической защиты ПДн, обеспечиваемый СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу.

Вывод:

Анализ возможностей потенциального нарушителя, проведенный с учетом комплекса организационно-режимных мер, реализованных в ИСПДн «НГАУ», показал, что потенциальный нарушитель относится к нарушителям типа Н1.

В соответствии с «Методическим рекомендациям по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных 8 Центром ФСБ России от 21.02.2008 № 149/54-144, при отнесении потенциального нарушителя к типу Н1 должна обеспечиваться криптографическая защита ПДн по уровню КС1.

6.1.1.9 Определение требуемого класса СКЗИ

Определение требуемого класса СКЗИ осуществляется на основании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и с учетом типа актуальных угроз (в соответствии с приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»). Таким образом, в соответствии с определенным УЗ ПДн (4 (четвертый) УЗ для ИСПДн) и типом актуальных угроз (угрозы 3 типа) в ИСПДн могут применяться СКЗИ класса КС1 и выше.

Вывод:

На основании п. 6.1.1.8, а также с учетом изложенных предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, в ИСПДн «НГАУ» рекомендуется применять СКЗИ класса КС1.

6.1.2.Аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными.

Конструктивно встроенные аппаратные закладки создаются в ходе проектирования и разработки аппаратного обеспечения, применяемого в ИС, и могут проявляться в виде НДВ различных элементов вычислительной системы.

Автономные аппаратные закладки являются законченными устройствами, выполняющими определенные функции перехвата, накопления, передачи или ввода/вывода информации, и могут внедряться во время эксплуатации ИС. Например, функции автономной аппаратной закладки может выполнять сотовый телефон, несанкционированно подключаемый к ТС ИС.

Учитывая, что аппаратные закладки представляют собой некоторый элемент ТС, скрытно внедряемый или подключаемый к ИС и обеспечивающий при определенных условиях реализацию НСД или непосредственное выполнение некоторых деструктивных действий, в них, как правило, содержатся микрокоманды, обеспечивающие взаимодействие закладки с программными и техническими средствами ИС. Аппаратные закладки могут реализовать угрозы:

- сбора и накопления информации, обрабатываемой и хранимой в ИС;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации ТЗИ на всех стадиях (этапах) жизненного цикла ИС.

Вывод:

Наличие аппаратной закладки в составе ИСПДн маловероятно в связи с высокой стоимостью аппаратных закладок и сложности их скрытой установки при организационно-режимных мероприятиях, реализованных на ОИ.

ТС, участвующие в обработке и передаче ПДн, закупаются у официальных дистрибьюторов и надежных, проверенных поставщиков, в связи с чем, вероятность внедрения

конструктивно встроенных аппаратных закладок считается крайне низкой. Неконтролируемое пребывание посторонних лиц в КЗ, где установлены ТС ИСПДн, маловероятно, в связи с чем, вероятность установки автономных аппаратных закладок посторонними лицами крайне низка.

Таким образом, аппаратная закладка не рассматривается как источник УБПДн.

6.1.3 Носитель вредоносной программы

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;
- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в ПО, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

- программные закладки (программа типа «Троянский конь»);
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

Троянская программа – вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно.

Троянские программы распространяются людьми – как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах. Во втором случае троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов.

Троянская программа может имитировать имя и иконку существующей или несуществующей и привлекательной программы, компонента или файла данных (например, картинки) как для запуска пользователем, так и для маскировки в системе своего присутствия.

Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Компьютерный вирус – разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды – например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном ПО (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т.д.) вместе с эксплоитом, использующим уязвимость.

Сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Сетевые черви проникают на компьютер без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в ПО и ОС, чтобы проникнуть на компьютер. Уязвимости – это ошибки и недоработки в ПО, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в ОС и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет.

Вывод:

Преднамеренное внедрение вредоносных программ в ИСПДн в процессе разработки, установки и настройки ПО исключено, так как системное и прикладное ПО, применяемое в ИСПДн, устанавливается с оригинальных лицензионных дисков, закупленных у официальных дистрибьюторов или надежных поставщиков.

Возможно случайное внедрение программных закладок и вирусов в процессе разработки, установки, настройки, сопровождения и эксплуатации ИСПДн, также велика вероятность внедрения вредоносной программы в ИСПДн по сети.

Наличие вредоносной программы может нанести значительный вред ИСПДн, таким образом, вредоносная программа рассматривается как источник УБПДн.

6.2 Уязвимости информационной системы

6.2.1 Причины возникновения уязвимостей

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки ПО, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

6.2.2 Актуальность уязвимостей в информационной системе персональных данных

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной ИСПДн, которые могут быть использованы для реализации УБПДн.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

- неправильные настройки ПО, неправомерное изменение режимов работы устройств и программ;

- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

6.2.2.1 Уязвимости программного обеспечения

1) Уязвимости системного ПО необходимо рассматривать с привязкой к архитектуре построения вычислительных систем.

При этом возможны уязвимости:

- в микропрограммах, в прошивках ПЗУ, ППЗУ;

- в средствах ОС, предназначенных для управления локальными ресурсами ИС (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;

- в средствах ОС, предназначенных для выполнения вспомогательных функций: утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т.п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.д.);

- в средствах коммуникационного взаимодействия (сетевых средствах) ОС.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для НСД без обнаружения таких изменений ОС;

- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

- отсутствие необходимых СЗИ (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

2) Уязвимости прикладного ПО.

К прикладному ПО относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), СУБД, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), СЗИ общего пользования и т.п.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной ИС (в том числе программные СЗИ, разработанные для конкретной ИС).

Уязвимости прикладного ПО могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИС и вызова штатных функций ОС, выполнения НСД без обнаружения таких изменений ОС;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых СЗИ (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности НСД к информации.

Вывод:

К актуальным уязвимостям системного ПО следует отнести уязвимости в микропрограммах, драйверах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, представляющие собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для НСД без обнаружения таких изменений ОС;
- отсутствие необходимых СЗИ (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Прикладное ПО в ИСПДн устанавливается с оригинальных лицензионных дисков, закупленных у официальных дистрибьюторов или надежных поставщиков. К актуальным уязвимостям прикладного ПО следует отнести уязвимости, представляющие собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и вызова штатных функций ОС, выполнения НСД без обнаружения таких изменений ОС;
- отсутствие необходимых СЗИ (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности НСД к ПДн.

Уязвимости специального ПО связаны только с возникновением угроз в результате сбоев в работе, отказов программно-аппаратных средств, которые описаны в п. 6.2.2.5.

6.2.2.2 Уязвимости, вызванные наличием в информационной системе аппаратной закладки

Аппаратная закладка как источник угроз не рассматривается в ИСПДн, следовательно, уязвимости, вызванные наличием в ИСПДн аппаратной закладки, не актуальны.

6.2.2.3 Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Вывод:

Рассматриваются уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных. Угрозы, связанные с каналами передачи данных, актуальны в условиях прохождения каналов связи вне КЗ.

6.2.2.4 Уязвимости, вызванные недостатками организации технической защитой информации от несанкционированного доступа

Защитные механизмы ПО не обеспечивают необходимый уровень защищенности ИСПДн (аутентификацию, проверку целостности, проверку форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.). Уязвимости, вызванные недостатками организации ТЗИ от НСД, рассматриваются как актуальные.

6.2.2.5 Уязвимости программно-аппаратных средств информационной системы в результате сбоев в работе, отказов этих средств

Уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств, не рассматриваются. В ИСПДн используются источники бесперебойного питания, обеспечивающие электропитание компьютерной системы и оборудования во время перепада напряжения в электрической сети.

6.2.2.6 Наличие технических каналов утечки информации

За счет использования ТКУИ возможно возникновение следующих угроз безопасности:

1) Утечка акустической (речевой) информации.

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

Утечка акустической (речевой) информации может быть осуществлена:

- с помощью аппаратных закладок;
- за счет съема виброакустических сигналов;
- за счет излучений, модулированных акустическим сигналом (микрофонный эффект и ВЧ излучение);
- за счет оптического излучения, модулированного акустическим сигналом.

2) Утечка видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра защищаемой информации с помощью оптических (оптикоэлектронных) средств с экранов мониторов и других устройств отображения, входящих в состав ИС (устройства отображения СВТ, информационно-вычислительных комплексов, ТС обработки графической, видео- и буквенно-цифровой информации). Кроме этого, просмотр (регистрация) информации возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений. Необходимым условием осуществления просмотра (регистрации) информации является наличие прямой видимости между средством наблюдения и носителем информации.

Утечка видовой информации может быть осуществлена:

- за счет удаленного просмотра экранов мониторов и других средств отображения информации;

- с помощью аппаратных закладок (скрытых устройств видеонаблюдения).

3) Утечка информации по каналам ПЭМИН.

Возникновение угрозы утечки защищаемой информации по каналам ПЭМИН возможно за счет перехвата ТС побочных (не связанных с прямым функциональным назначением) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации ТС ИС. Генерация информации, содержащей защищаемую информацию и циркулирующей в ТС ИС в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях ТС ИС сопровождаются побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИС. Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в ТС ИС. Для этого используются радиоприемные устройства и оконечные устройства восстановления информации.

Утечка информации по каналам ПЭМИН может быть осуществлена:

- за счет побочных электромагнитных излучений электронно-вычислительной техники;

- за счет наводок по цепям электропитания;

- за счет радиоизлучений, модулированных информационным сигналом.

Вывод:

Угрозы утечки акустической (речевой) и видовой информации в ИСПДн исключены, так как в ИСПДн отсутствует речевой ввод информации и в помещении ИСПДн отсутствуют окна.

Предполагается, что в число возможных каналов атак не входят каналы утечки за счет ПЭМИН в связи с малой результативностью, трудоемкостью и высокой ценой. При этом все оборудование, необходимое для функционирования ИСПДн, находится в пределах КЗ. Приняты организационные меры, при которых неконтролируемое пребывание посторонних лиц в служебных помещениях маловероятно.

6.2.2.7 Уязвимости средств защиты информации

В ИСПДн применяются только сертифицированные по требованиям безопасности СЗИ, в том числе СКЗИ. Поэтому, уязвимости СЗИ, не рассматриваются, и принимаются как неактуальные.

6.3 Способы реализации угроз в информационной системе

Можно выделить следующие способы реализации угроз в ИС.

1) Использование существующих уязвимостей программно-аппаратного обеспечения ИС, позволяющих:

- Вскрывать или перехватывать пароли.

- Обходить СЗИ.

- Деструктивно воздействовать на СЗИ.

- Использовать остаточную, неучтенную информацию (сбор «мусора»).

- Использовать нетрадиционные (стенографические) каналы передачи информации.

- Использовать уязвимости протоколов сетевого взаимодействия и каналов передачи данных, позволяющих:

а) перехватывать информацию;

б) модифицировать передаваемые данные;

в) перегружать ресурсы в ИС (отказ в обслуживании);

г) внедрять вредоносные программы;

д) получать удалённый НСД к системе,

е) разглашать и организовывать утечку информации на незащищённые рабочие места.

2) Внедрение (внесение) новых уязвимостей в ИС на этапе проектирования, разработки и сопровождения ИС:

- Использование нештатного ПО.

- Внесение уязвимостей с использованием штатных средств:

а) обмен программами и данными, содержащими выполняемые модули (скрипты, макросы и т.д.);

б) изменение конфигурации ПО и данных;

в) модификация ПО и данных;

г) разработка вредоносных программ;

д) публикация, разглашение защищаемой информации.

6.4 Объект воздействия в информационной системе

Объектом воздействия могут быть:

1) Информация, обрабатываемая на ТС (узле) ИС, находящаяся:

- на отчуждаемых носителях (на гибких магнитных дисках, на жёстких магнитных дисках, на накопителях ZIP, на накопителях электронной памяти типа флеш, на аудио-, видеокассетах, магнитных лентах, на оптических компакт-дисках, в сотовых телефонах, карманных компьютерах, цифровых фотоаппаратах, mp3-проигрывателях, в цифровых видеокамерах, и в других устройствах);
- на встроенных носителях долговременного хранения информации (на жёстких магнитных дисках, в ПЗУ, на ППЗУ);
- в средствах обработки и хранения оперативной информации (в оперативной памяти, в кеш-памяти, в буферах ввода/вывода информации, в видео-памяти, в оперативной памяти подключаемых устройств).

2) Информация в средствах, реализующих сетевое взаимодействие, и каналах передачи данных в сети:

- в маршрутизаторах;
- в других устройствах коммутации.

Вывод:

Для ИСПДн объектами воздействия могут являться:

- аппаратное обеспечение,
- прикладное ПО,
- сетевое ПО,
- сетевой трафик,
- сетевой узел,
- системное ПО,
- учётные данные пользователя.

6.5 Деструктивное действие к информации в информационной системе

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

Нарушение конфиденциальности может быть осуществлено в случае утечки информации:

- копирования ее на отчуждаемые носители информации;
- передачи ее по каналам передачи данных;
- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- разглашения (публикация) защищаемой информации;
- кража (повреждение) ТС ИС.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

- микропрограммы, данные и драйвера устройств вычислительной системы;
- программы, данные и драйвера устройств, обеспечивающих загрузку ОС;
- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) ОС;

- программы и данные прикладного ПО;
- программы и данные специального ПО;
- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в ИС может также быть вызвано внедрением в нее вредоносной программы или воздействием на систему защиты информации или ее элементы.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

7 Определение показателей угроз безопасности персональных данных ИСПДн «НГАУ»

7.1 Определение уровня исходной защищенности

Уровень исходной защищенности (Y1) ИСПДн определяется экспертным методом в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных» (далее – Методика), утвержденной от 14.02.2008 заместителем директора ФСТЭК России. Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 3 для ИСПДн.

Таблица 3. Технические и эксплуатационные характеристики ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень исходной защищенности			ИСПДн «НГАУ»
	Высокий	Средний	Низкий	
1 По территориальному размещению:				Высокий
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			✓	
городская ИСПДн, 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		✓		
локальная ИСПДн, развернутая в пределах одного здания	✓			
2 По наличию соединения с сетями общего пользования:				Средний
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 БД:				Низкий
чтение, поиск	✓			
запись, удаление, сортировка		✓		
модификация, передача			✓	
4 По разграничению доступа к данным:				Средний
ИСПДн, к которой имеет доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн		✓		
ИСПДн, к которой имеют доступ все сотрудники			✓	

Технические и эксплуатационные характеристики ИСПДн	Уровень исходной защищенности			ИСПДн «НГАУ»
	Высокий	Средний	Низкий	
организации, являющейся владельцем ИСПДн				
ИСПДн с открытым доступом			✓	
5 По наличию соединений с другими базами иных ИСПДн:				Высокий
интегрированная ИСПДн (организация использует несколько баз данных, при этом организация не является владельцем всех используемых баз)			✓	
ИСПДн, в которой используется одна база, принадлежащая организации – владельцу данной ИСПДн	✓			
6 По уровню обобщения (обезличивания) ПДн:				Низкий
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			✓	
7 По объему данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:				Низкий
ИСПДн, предоставляющая всю БД			✓	
ИСПДн, предоставляющая часть данных		✓		
ИСПДн, не предоставляющие никакой информации	✓			

Исходная степень защищенности (Y1) определяется следующим образом:

- ИСПДн имеет высокий уровень исходной защищенности (Y1 = 0), 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).
- ИСПДн имеет средний уровень исходной защищенности (Y1 = 5), если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности.
- ИСПДн имеет низкую степень исходной защищенности (Y1 = 10), если не выполняются условия по двум пунктам выше.

Вывод:

ИСПДн «НГАУ» имеет низкий уровень исходной защищенности (Y1 = 10).

7.2 Методика определения актуальности угроз безопасности персональных данных

Частота реализации УБПДн (Y2) определяется экспертным методом в соответствии с Методикой и на основании результатов обследования ИСПДн. Возможные значения частоты реализации угроз приведены в Таблице 4.

Таблица 4. Частоты реализации угроз

Вероятность	Описание
Маловероятно (Y2 = 0)	Отсутствуют объективные предпосылки для осуществления угрозы, т.е. отсутствует источник угрозы или уязвимое звено (например, угроза утечки речевой информации при отсутствии в ИСПДн функций голосового ввода защищаемой информации).
Низкая вероятность (Y2 = 2)	Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие СЗИ).
Средняя вероятность (Y2 = 5)	Объективные предпосылки для реализации угрозы существуют, принятые меры обеспечения безопасности защищаемой информации недостаточны.
Высокая вероятность (Y2 = 10)	Объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности защищаемой информации не приняты.

Вывод:

Перечень УБПДн, актуальных для ИСПДн «НГАУ», представлен в Модели угроз. Перечень составлен в соответствии с Банком данных угроз безопасности информации ФСТЭК России с учётом структурно-функциональных характеристик ИСПДн, применяемых информационных технологий и особенностей (условий) функционирования ИС, а так же определенного в п.6.1.1.4 потенциального нарушителя безопасности ПДн – внутренний нарушитель с низким потенциалом.

8 Заключение

Актуальные УБПДн, установленные в ходе изучения ИСПДн, представляют собой условия и факторы, создающие реальную опасность НСД к ПДн с целью нарушения 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 являются неактуальными.

Угрозы хищения, разрушения, несанкционированного копирования или уничтожения носителей информации нейтрализуются совершенствованием системы охраны, пропускного режима, делопроизводства, а также изменением режима обращения с носителями информации, содержащими ПДн.

Угрозы, связанные с использованием недокументированных возможностей ПО признаны маловероятными, в связи с тем, что отсутствуют объективные предпосылки для реализации данных угроз.

Угрозы, связанные с нарушением конфиденциальности при передачи ПДн по сети признаны маловероятными, в связи с тем, что в ИСПДн построена с использованием VPN-канала (сертифицированных СКЗИ).

Для нейтрализации остальных актуальных угроз необходимо создание СЗПДн с применением дополнительных СЗИ.

Структура, состав и основные функции СЗПДн определяются исходя из характеристик и требований на основе приказа ФСТЭК России от 18.02.2013 № 21 и постановления Правительства РФ от 01.11.2012 № 1119 с учетом последствий, которые могут наступить в результате нарушения заданных характеристик безопасности информации в случае возникновения актуальных УБПДн. При этом система защиты должна состоять из организационных мер и СЗИ (в том числе СКЗИ), а также из используемых в ИСПДн информационных технологий, и должна обеспечивать нейтрализацию (блокирование) УБПДн, связанных с действиями нарушителя с низким потенциалом. К нарушителям с низким потенциалом для ИСПДн относятся внешний нарушитель.

В целях обоснованного подхода к обеспечению безопасности ПДн для нейтрализации актуальных угроз, выявленных согласно вышеизложенной Модели угроз, в составе мероприятий по защите информации целесообразно использовать следующие мероприятия:

- по идентификации и аутентификации субъектов доступа и объектов доступа;
- по управлению доступом субъектов доступа к объектам доступа;
- по регистрации событий безопасности;
- по антивирусной защите;
- по контролю (анализу) защищённости информации;
- по защите технических средств;
- по защите информационной системы, ее средств, систем связи и передачи данных.

Подпись разработчика:

Проректор по лицензированию, аккредитации и ИТ *Наумкин И.В.* /
(Должность, ФИО) (подпись)

Директор ЦИТ *Каракулов А.В.* /
(Должность, ФИО) (подпись)

ЛИСТ РАССЫЛКИ

№ п/п	Наименование подразделения	Номер экземпляра	Подпись и расшифровка подписи должностного лица, получившего док.	Примечание

Подпись лица, произведшего рассылку _____ / /
(Должность, ФИО) (подпись)

Дата рассылки «____» _____ 20 г.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номера страниц				№ "Извещения об изменении"	Дата введения изменения, № приказа и дата	Подпись
	измененных	замененных	новых	аннулированных			

ЛИСТ ОЗНАКОМЛЕНИЯ

Дата ознакомления	Наименование должности	Подпись	Расшифровка подписи	Номер изменения