УТВЕРЖДАЮ

Директор МБОУ КСОШ № 19

М.Ф. Филь

М.П.

«08» июля 2016

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
при их обработке на автоматизированном рабочем месте оператора государственной информационной системы «Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования» муниципального бюджетного общеобразовательного учреждения казачьей средней общеобразовательной школы № 19

СОГЛАСОВАНО:

Заместитель директора по УВР	(подпись)	Л.А. Бадминова
Учитель математики и информатики	(подпись)	Т.Н. Алфимова
Заместитель директора по УВР	(подпись)	М.А. Олейникова

2016 год

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ЕИС ПГиМУ СО	Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
МО	Медицинская организация
НЖМД	Накопитель на жестких магнитных дисках
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПТС	Программно-технические средства
ПЭВМ	Персональная электронно-вычислительная машина
ПЭМИН	Побочные электромагнитные излучения и наводки
СВТ	Средства вычислительной техники
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
ТКУИ	Технические каналы утечки информации
ТС	Технические средства
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Атака	Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)
Безопасность персональных данных	Состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных
Вирус (компьютерный, программный)	Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению
Внешняя информационная система	Информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора
Внешняя информационно-телекоммуникационная сеть	Информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы
Доступ в информационную среду компьютера (информационной системы персональных данных)	Получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ
Доступ к информации	Возможность получения информации и её использования
Доступность	Состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Защищенные линии связи	Линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или)

	доступность)
Идентификатор	Представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе
Идентификация	Присвоение субъектам и объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Инцидент	Непредвиденное или не желательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)
Канал атаки	Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) осуществляемых при проведении атаки действий
Категория доступа к информации	Показатель, в зависимости от которого информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)
Контролируемая зона	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 выполнения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания
Модель нарушителя	Совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности
Модель угроз	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности персональных данных
Нарушитель безопасности персональных данных	Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных

	системах персональных данных
Недекларированные возможности	Функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами
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
Отказ в обслуживании	Препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы
Персональные данные	Любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)
Побочные электромагнитные излучения и наводки	Электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания
Пользователь информационной системы	Лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования
Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Программная закладка	Код программы, преднамеренно внесённый в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и(или) блокировать аппаратные средства
Ресурс информационной системы	Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы
Роль	Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и

	информационной системой
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
Субъект доступа	Пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа
Технические средства	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации
Технический канал утечки информации	Совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация
Угрозы безопасности персональных данных	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных
Уничтожение персональных данных	Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных
Управление доступом	Ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
Уязвимость	Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации
Целостность информации	Состояние информации, при котором её изменение осуществляется только преднамеренно субъектами, имеющими на него право

ВВЕДЕНИЕ

Настоящий документ (далее по тексту – Модель) описывает возможные угрозы безопасности персональных данных, которым подвержено автоматизированное рабочее место оператора государственной информационной системы «Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования» (далее по тексту – АРМ оператора ЕИС ПГиМУ СО) муниципального бюджетного общеобразовательного учреждения казачьей средней общеобразовательной школы № 19 (далее по тексту – Учреждение).

Модель, учитывая особенности АРМ оператора ЕИС ПГиМУ СО, используемые технические средства и технологические процессы обработки информации, в т.ч. персональных данных (далее по тексту – ПДн), позволяет определить конкретные условия эксплуатации, защищаемые информационные ресурсы, дать описания угроз безопасности информации, которым подвержено АРМ оператора ЕИС ПГиМУ СО.

Разработка Модели велась на основании анализа исходных данных по объекту информатизации, законодательства Российской Федерации, нормативных и правовых документов органов исполнительной власти с учётом требований по обеспечению безопасности информации, в т.ч. ПДн.

При разработке Модели применяется риск-ориентированный подход, при котором определяется перечень актуальных угроз безопасности персональных данных, и на их основе в дальнейшем разрабатывается система защиты информации (далее по тексту – СЗИ) АРМ оператора ЕИС ПГиМУ СО.

Средства защиты информационных ресурсов и технических средств АРМ оператора ЕИС ПГиМУ СО, входящие в состав СЗИ, должны осуществлять защиту от влияния как преднамеренных, так и случайных событий, процессов или явлений, приводящих к несанкционированному доступу к информации, а также возможности воздействия на компоненты АРМ оператора ЕИС ПГиМУ СО, приводящие к сбою их функционирования и возникновению различных негативных последствий в отношении ресурсов СЗИ.

Модель разработана на основе методических документов ФСТЭК России и ФСБ России:

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);

«Состав и содержание 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» (утверждены приказом ФСБ России от 10 июля 2014 г. № 378);

«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432).

Угрозы безопасности персональных данных (далее по тексту – УБПДн), содержащиеся в настоящей Модели, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБИ на АРМ оператора ЕИС ПГиМУ СО.

Для обеспечения актуальности Модели должен осуществляться ее плановый (регулярный) и внеплановый пересмотр.

Плановый пересмотр проводится в порядке проведения контроля состояния обеспечения защиты информации, в т.ч. ПДн (не реже одного раза в год).

Внеплановый пересмотр должен осуществляться в случаях:

изменения требований законодательства Российской Федерации в области защиты информации, нормативно-правовых актов и методических документов, регулирующих защиту персональных данных;

изменения конфигурации и условий размещения АРМ оператора ЕИС ПГиМУ СО;

изменения в составе основных элементов АРМ оператора ЕИС ПГиМУ СО, которые могут повлиять на состав УБИ.

1 ОПИСАНИЕ СИСТЕМЫ

1.1 Конфигурация информационной системы

Информационная система представляет собой автоматизированное рабочее место, являющееся частью IT-инфраструктуры Учреждения, и предназначенное для взаимодействия с государственной информационной системой «Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования».

Технические средства АРМ оператора ЕИС ПГиМУ СО расположены по адресу: 357560, Ставропольский край, г. Пятигорск, пос. Горячеводский, ул. Ленина, 25, 2 этаж, методический кабинет.

Границей контролируемой зоны (КЗ) АРМ оператора ЕИС ПГиМУ СО являются ограждающие конструкции помещения, в котором расположены технические средства объекта информатизации.

На рисунке 1 представлена структурная схема АРМ оператора ЕИС ПГиМУ СО.

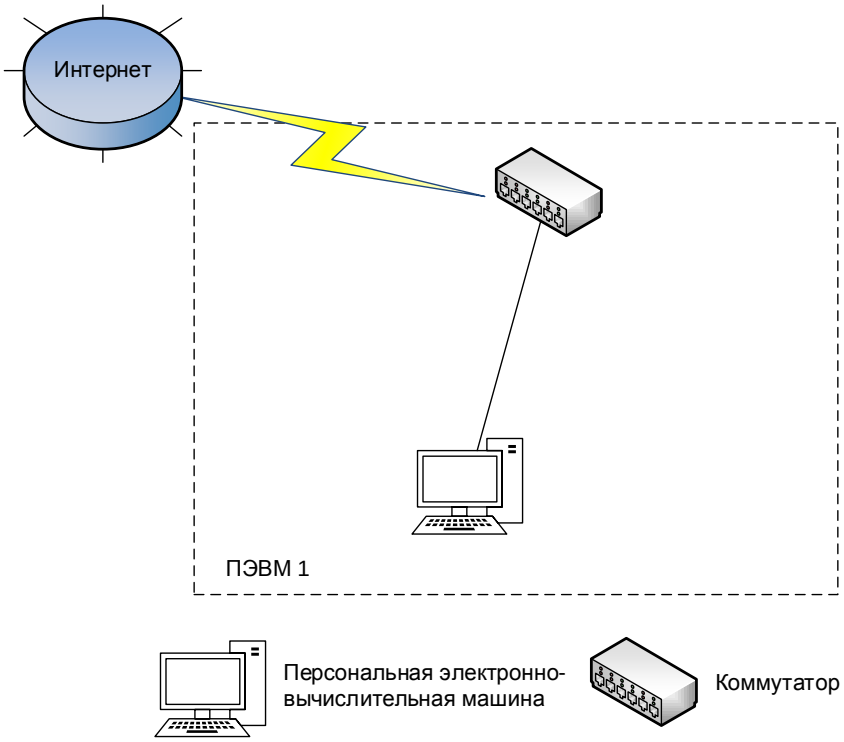

Рисунок 1 – Структурная схема информационной системы

1.2 Структурные элементы информационной системы

В состав информационной системы входят следующие структурные элементы:

а) программно-технические средства обработки:

общесистемное и специальное программное обеспечение, участвующее в обработке информации, в т.ч. ПДн;

средства и утилиты системы управления ресурсами информационной системы;

аппаратные средства обработки информации, в т.ч ПДн;

б) средства защиты информации:

средства управления доступом пользователей (встроенные в ОС);

средства обеспечения регистрации и учета действий с информацией (встроенные в ОС);

средства, обеспечивающие целостность данных (встроенные в ОС);

средства антивирусной защиты;

в) каналы информационного обмена и телекоммуникации;

г) объекты и помещения, в которых размещены компоненты информационной системы.

1.3 Состав и структура информации, обрабатываемой в информационной системе

Обработка информации на АРМ оператора ЕИС ПГиМУ СО осуществляется в соответствии с Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», письмом Минобрнауки России от 15.02.2012 №АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде», распоряжением Правительства РФ от 28.12.2011 №2415-р «О государственных и муниципальных услугах, предоставляемых в электронном виде» и другими нормативно-правовыми актами.

Состав персональных данных сотрудников, обрабатываемых на АРМ оператора ЕИС ПГиМУ СО:

- фамилия, имя, отчество;
- место, год и дата рождения;
- пол;
- адрес по прописке;
- адрес фактического проживания;
- паспортные данные (серия, номер паспорта, кем и когда выдан);
- информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- телефонный номер (домашний, рабочий, мобильный);
- семейное положение и состав семьи (муж/жена, дети);
- гражданство;
- информация о знании иностранных языков;
- данные о трудовом договоре;
- ИНН;
- данные полиса обязательного медицинского страхования;
- данные свидетельства государственного пенсионного страхования;
- данные об аттестации работников;
- данные о повышении квалификации;
- данные о наградах, медалях, поощрениях, почетных званиях;
- информация о приеме на работу, перемещении по должности, увольнении;
- информация об отпусках;
- информация о командировках;
- информация о болезнях;
- информация о негосударственном пенсионном обеспечении;
- логин, пароль, роль для работы в ЕИС ПГиМУ СО.

Состав персональных данных обучающихся:

- фамилия, имя, отчество;
- дата и место рождения;
- сведения о близких родственниках (фамилия, имя, отчество, дата рождения, серия и номер документа, удостоверяющего личность, кем и когда выдать);
- адрес места регистрации и места фактического проживания;
- данные документа, удостоверяющего личность (свидетельство о рождении, паспорт), (серия, номер, кем и когда выдан);

- данные полиса обязательного медицинского страхования (серия, номер, когда и кем выдан);
- СНИЛС;
- сведения об успеваемости;
- номер личного дела;
- дополнительные данные, сообщаемые в заявлении о приеме в образовательную организацию.

Сведения о национальности, состоянии здоровья, биометрические данные и иные данные, относящиеся к специальным категориям персональных данных, в информационную систему не вносятся.

На основании состава обрабатываемых ПДн можно сделать вывод, что на АРМ оператора ЕИС ПГиМУ СО осуществляется обработка иных категорий ПДн субъектов ПДн, являющихся и не являющихся сотрудниками оператора. Количество субъектов ПДн, не являющихся сотрудниками оператора – менее 100000.

1.4 Режим обработки информации

Ввод данных на АРМ оператора ЕИС ПГиМУ СО осуществляется уполномоченными сотрудниками Учреждения.

Режим обработки предусматривает следующие действия с персональными данными: сбор, запись, систематизация, уточнение (обновление, изменение), поиск, сортировка, передача.

На АРМ оператора ЕИС ПГиМУ СО обработка информации осуществляется в многопользовательском режиме. Пользователи имеют права доступа к защищаемой информации в соответствии с ролью, присвоенной в ЕИС ПГиМУ СО. Разграничение прав доступа предполагается предусмотреть только к настройкам средств защиты информации.

Все пользователи АРМ оператора ЕИС ПГиМУ СО имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 1.

Таблица 1 – Матрица доступа

Группа	Уровень доступа к информации (ПДн)	Разрешенные действия	Сотрудники отдела
Администраторы информационной системы	Обладает полной информацией о системном и прикладном программном обеспечении ИС. Обладает полной информацией о технических средствах и конфигурации ИС. Имеет доступ ко всем техническим средствам обработки информации и данным ИС. Обладает правами конфигурирования и административной настройки технических средств ИС.	Настройка, администрирование элементов и ПО ИС	Олейникова Марина Александровна Заместитель директора по УВР
Операторы информационной системы	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн.	Сбор, запись, систематизация, уточнение (обновление, изменение), поиск, сортировка, передача	Заместители директора Учителя

2 МОДЕЛЬ НАРУШИТЕЛЯ

2.1 Описание нарушителей

С точки зрения наличия права постоянного или разового доступа в контролируемую зону объектов размещения информационной системы все физические лица могут быть отнесены к двум категориям:

категория I – лица, не имеющие права доступа в контролируемую зону информационной системы;

категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы (далее по тексту – ИС).

Все потенциальные нарушители подразделяются на:

внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИС;

внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИС.

Внешними нарушителями могут быть как лица категории I, так и лица категории II. Внутренними нарушителями могут быть только лица категории II.

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;

нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;

проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа программного обеспечения прикладного программного обеспечения (далее по тексту – ПО) и средств защиты информации, не является целесообразным для нарушителей с учетом высокой стоимости разработки способов и средств атаки.

2.1.1 Внешние нарушители

Внешний нарушитель не имеет свободного доступа к системам и ресурсам ИС, находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также через технические каналы утечки информации.

Нарушители данного вида при создании способов, подготовке и проведении атак могут использовать возможности из числа следующих:

- осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи; проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи; проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой штатными средствами ИС, проводить попытки навязывания ложной информации; проводить попытки внедрения вредоносного ПО; проводить атаки с целью вызвать отказы в работе отдельных компонентов ИС;

- применять находящиеся в свободном доступе источники (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используются средства криптографической защиты информации. При этом может быть получена следующая информация: общие сведения об информационной системе (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); сведения об информационных технологиях, базах данных, ПО, используемых в информационной

системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии; содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ; общие сведения о защищаемой информации; сведения о каналах связи, по которым передаются персональные данные.

Нарушители данного вида не могут использовать для реализации атак штатные средства ИС.

Средства атаки, доступные данной категории нарушителя:

доступные в свободной продаже технические средства (далее по тексту – ТС) и ПО.

Данная категория нарушителей обладает только доступной из открытых источников информацией о применяемых в ИС технических средствах.

Лица данной категории не являются доверенными.

2.1.3 Внутренние нарушители

К **первой группе** относятся сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам ИС, но имеющие санкционированный доступ в контролируемую зону (далее по тексту – КЗ). К этой категории нарушителей относятся сотрудники Учреждения, рабочие места которых находятся в помещениях с техническими средствами ИС, а также технический и вспомогательный персонал: электрики, сантехники, уборщицы и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

При создании способов, подготовке и проведении атак нарушители данного типа могут использовать возможности из числа следующих:

- получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация: общие сведения об информационной системе (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); сведения об информационных технологиях, базах данных, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии; содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ; общие сведения о защищаемой информации; сведения о каналах связи, по которым передается защищаемая информация;

- получение в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС; сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИС; сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

Средства атаки, доступные данной категории нарушителя:

доступные в свободной продаже ТС и ПО.

Использование штатных средств ограничено мерами, реализованными в ИС и направленными на предотвращение и пресечение несанкционированных действий.

Лица данной категории не являются доверенными, но нахождение лиц данной группы в помещениях с элементами ИС, в силу принятых организационных мер возможно только при наблюдении ответственных лиц Учреждения, что делает невозможным проведение атаки. Поэтому лиц данной категории можно исключить из числа актуальных нарушителей ИБ ИС.

Ко **второй группе** относятся зарегистрированные пользователи ИС осуществляющие ограниченный доступ к ресурсам ИС с рабочего места.

Лицо данной группы:

обладает всеми возможностями лиц первой группы;

знает, по меньшей мере, одно легальное имя доступа;

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ИР ИС;

располагает ресурсами, к которым имеет доступ;

имеет возможность прямого (физического) доступа к отдельным техническим средствам ИС.

Средства атаки, доступные данной категории нарушителя:

доступные в свободной продаже ТС и ПО;

штатные средства.

С учетом того, что СЗИ не может обеспечить ее защиту от действий, выполняемых в рамках предоставленных рассматриваемой группе нарушителей полномочий (например, защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации), и исходя из анализа реализованных в ИС административно-организационных мер безопасности в отношении персонала, допущенного для работы в ИС, при построении модели нарушителя использовалось предположение о доверенности пользователей ИС, которые имеют санкционированный доступ к защищаемой информации (персональным данным), доступ к ключевой информации, а также обладают знаниями о технологии обработки информации и системе принимаемых мер защиты.

Доверенность данной категории лиц означает, что они не являются злоумышленниками, т.е. не предпринимают умышленных действий (бездействия) при выполнении своих должностных обязанностей, могущих привести к реализации угроз безопасности информации. Поэтому в дальнейшем указанные лица не рассматриваются в качестве потенциальных нарушителей.

К **третьей группе** относятся зарегистрированные пользователи с полномочиями администратора безопасности ИС, выполняющие обслуживание и поддержку эксплуатации ИС, контроль за комплексом технических средств, ПО системы и СрЗИ.

Лицо данной группы:

обладает всеми возможностями лиц второй группы;

обладает полной информацией о системном и прикладном ПО, используемом в ИС;

обладает полной информацией о технических средствах и конфигурации ИС;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в ИС;

имеет доступ ко всем техническим средствам и данным ИС;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств ИС.

Средства атаки, доступные данной категории нарушителя:

штатные средства;

доступные в свободной продаже ТС и ПО.

Лица данной категории обладают полными знаниями об ИС.

Учитывая выполняемые функции, степень возложенной на них ответственности и высокий уровень их квалификации, лица, отнесенные к данной категории, проходят специальный отбор, в их отношении ведется непрерывный контроль. Лица данной категории выполняют все внутренние требования, регламенты и инструкции по обеспечению информационной, производственной и пожарной безопасности, регулярно проходят необходимый инструктаж.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить администраторов безопасности из числа актуальных нарушителей информационной безопасности (далее по тексту – ИБ) ИС.

К **четвертой группе** относятся лица из числа программистов-разработчиков сторонних организаций, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИС.

Лицо данной группы:

обладает информацией об алгоритмах и программах обработки информации в ИС;

обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИС на стадии разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИС.

Средства атаки, доступные данной категории нарушителя:

штатные средства;

доступные в свободной продаже ТС и ПО.

В отношении сотрудников сторонних организаций, привлекаемых к обслуживанию ИС на основании договора, проводятся проверки по линии безопасности, благонадежность этих сотрудников подтверждается организацией-работодателем, в их отношении действуют документы, регламентирующие порядок обеспечения информационной безопасности и объектового режима. С компанией, привлекаемой к обслуживанию ИС, заключается соглашение о конфиденциальности. Сотрудники сторонних организаций действуют на объекте расположения ИС только в сопровождении и под непрерывным контролем ответственных сотрудников Учреждения.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить лиц данной группы из числа актуальных нарушителей ИБ ИС.

К **пятой группе** относится персонал сторонней организации, обеспечивающий поставку, сопровождение и ремонт ТС ИС.

Лицо данной группы:

обладает возможностями внесения закладок в ТС ИС на стадии их разработки, внедрения и сопровождения;

может располагать фрагментами информации о топологии ИС, автоматизированных рабочих местах, коммуникационном оборудовании, а также о средствах защиты информации, используемых в ИС.

Средства атаки, доступные данной категории нарушителя:

штатные средства;

доступные в свободной продаже ТС и ПО.

В отношении сотрудников сторонних организаций, привлекаемых к обслуживанию ТС ИС на основании договора, также проводятся проверки по линии безопасности, благонадежность этих сотрудников подтверждается организацией-работодателем, в их отношении действуют документы, регламентирующие порядок обеспечения информационной безопасности и объектового режима. С компанией, привлекаемой к обслуживанию ТС ИС, заключается соглашение о конфиденциальности. Сотрудники сторонних организаций действуют на объекте расположения ИС только в сопровождении и под непрерывным контролем ответственных сотрудников Учреждения.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить лиц данной группы из числа актуальных нарушителей ИБ ИС.

К **шестой группе** относятся лица, не являющиеся зарегистрированными пользователями системы, получившие разовый доступ в КЗ, в обязанности которых не входит обслуживание элементов ИС. Как правило, лица данной категории являются сотрудниками сторонних организаций, приглашенными на площадку объекта в деловых целях.

Средства атаки, доступные данной категории нарушителя:

доступные в свободной продаже ТС и ПО.

Данная категория нарушителей обладает только доступной из открытых источников информацией о применяемых в ИС технических средствах.

Лица данной категории не являются доверенными, но нахождение лиц данной группы на площадке объекта в силу принятых организационных мер возможно только под контролем ответственных лиц Учреждения. Поэтому лиц данной категории можно исключить из числа актуальных нарушителей ИБ ИС.

2.2 Предположение о возможности сговора нарушителей

В данном разделе рассмотрены предположения о возможности и характере сговора нарушителей и о возможности преимуществ, которыми могут располагать нарушители, находящиеся в сговоре.

Возможность сговора внутренних нарушителей между собой практически не даёт преимуществ сговорившимся нарушителям, помимо тех, которыми они обладают по отдельности. Кроме того, ввиду принятых на объекте информатизации организационно-технических мер, вероятность сговора данных категорий лиц маловероятна.

Возможность сговора внутренних нарушителей с любыми внешними нарушителями, с одной стороны, практически не даёт преимуществ сговорившимся нарушителям перед внутренним нарушителем, имеющим право постоянного или разового доступа в КЗ, действующим в одиночку. С другой стороны ввиду принятых на объекте организационно-технических мер, повышает вероятность обнаружения их противоправных действий.

С учётом изложенного выше, можно сделать вывод о том, что сговор между внешними и внутренними нарушителями не предоставляет им никаких дополнительных возможностей по сравнению с внутренним нарушителем, организующим и проводящим атаки, пользуясь доступом в контролируемую зону.

Возможность сговора внешних нарушителей между собой не предоставляет им никаких дополнительных возможностей по нарушению безопасности информации в ИС, помимо тех, которыми обладают по отдельности.

Таким образом, можно сделать вывод, что возможности нарушителей безопасности информации в ИС, существенно ограничиваются принятыми на объекте информатизации организационно-техническими мерами по обеспечению порядка доступа в помещения, в которых размещены технические средства обработки защищаемой информации ИС, в том числе используемыми средствами защиты информации, а также необходимыми защитными мерами и устройствами, реализованными в оборудовании и программном обеспечении ИС. Поэтому самостоятельно нарушители рассматриваемого типа могут осуществлять ограниченный набор действий, связанных с попытками доступа к информационным ресурсам ИС.

2.3 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

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 ТС и ПО, в том числе программные и аппаратные компоненты криптосредств.

Внутренний нарушитель для доступа к защищаемой информации может использовать штатные средства ИС. При этом его возможности по использованию перечисленных средств зависят от реализованных в ИС организационно-технических мер.

2.4 Описание каналов атак

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИС, являются:

каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);

штатные программно-технические средства ИС;

коммутационное оборудование, расположенное в пределах контролируемой зоны, не защищенное от НСД к информации организационно-техническими мерами; электронные носители, в том числе съемные, сданные в ремонт и вышедшие из употребления; неучтенные носители информации;

кабельные системы, расположенные в пределах контролируемой зоны, так и за ее пределами, не защищенные от НСД к информации организационно-техническими мерами.

2.5 Обобщенные возможности источников атак

На основании анализа исходных данных об ИС, объектах защиты и источниках атак определены обобщенные возможности источников атак. Обобщенные возможности источников атак представлены в таблице 2.

Таблица 2 - Обобщенные возможности источников атак

№ п/п	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	нет

2.6 Обоснование неактуальности угроз

В таблице 3 приводятся организационно-технические меры, направленные на противодействие возможностям источников атак.

Таблица 3 – Возможности нарушителей и меры противодействия угрозам атак

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; сотрудники, являющиеся пользователями ИС, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИС и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИС, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с защищаемой информацией, в т.ч. персональными данными; осуществляется контроль целостности средств защиты; на АРМ, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – элементы ИС), на которых реализованы СКЗИ и СФ.	не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения.
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений	не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагаются ресурсы ИС, обеспечивается в соответствии с контрольно-пропускным режимом;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.		сведения о физических мерах защиты объектов, в которых размещены элементы ИС, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Проводятся работы по подбору персоналов; помещения, в которых располагаются элементы ИС, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИС используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты.
2.1	Физический доступ к элементам ИС, на которых реализованы СКЗИ и СФ.	не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается элементы ИС, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются элементы ИС, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается элементы ИС, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения.
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается элементы ИС, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.		реализации возможности.
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

2.7 Основные организационно-технические меры, необходимые для противодействия возможностям источников атак

Реализация угроз безопасности информации, обрабатываемых в информационных системах определяется возможностями источников атак. Для противодействия возможностями источников атак в Учреждении должны быть приняты следующие организационно-технические меры:

на должности, в обязанности которых входят работа со средствами защиты, защищаемой информацией, назначаются ответственные добросовестные лица, имеющие положительные характеристики, ознакомленные с ответственность за несоблюдение правил обеспечения безопасности информации, имеющие знания и навыки в работе со средствами вычислительной техники и защиты информации.

организован контрольно-пропускной режим в помещения с элементами ИС и/или СКЗИ;

определен порядок доступа в помещения с элементами ИС и/или СКЗИ, лиц, не имеющих допуска к защищаемой информации;

помещения, в которых располагаются элементы ИС и/или СКЗИ, должны быть оснащены входными дверьми с замками;

обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

утверждены правила доступа в помещения, где располагаются элементы ИС и СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

назначены лица, отвечающие за администрирование информационной системы, безопасность информации и эксплуатацию СКЗИ;

утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;

документация на СКЗИ хранится у ответственного за СКЗИ в металлическом ящике;

осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

осуществляется регистрация и учет действий пользователей с защищаемой информацией;

осуществляется контроль целостности средств защиты;

на элементах ИС (АРМ), на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа и антивирусной защиты.

3 МОДЕЛЬ УГРОЗ

Модель угроз разрабатывается в соответствии с методологией ФСТЭК России, определённой в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года).

3.1 Идентификация уязвимых звеньев

Под уязвимым звеном подразумевается программное, аппаратное или программно-аппаратное средство, включая средства защиты информации, а также носители информации, в т.ч. ПДн, в отношении которых возможна реализация угроз НСД или утечки по техническим каналам.

Согласно «Методике определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы.

Таким образом, идентификация уязвимых звеньев необходима для идентификации всех принципиально реализуемых в информационной системе угроз безопасности.

3.1.1 Идентификация технических каналов утечки информации

При обработке информации, в т.ч. ПДн, возможно возникновение следующих угроз утечки информации по ТКУИ:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналам ПЭМИН.

Утечка акустической информации

Угроза утечки акустической (речевой) информации возможно при наличии функций голосового ввода информации, в т.ч. ПДн, в ИС или функций воспроизведения информации акустическими средствами ИС.

Утечка видовой информации

Реализация угрозы утечки видовой информации возможна за счет несанкционированного просмотра информации с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС.

Утечка по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, технических средств, входящих в состав ИС.

3.1.2 Идентификация уязвимых по отношению к НСД звеньев информационной системы

Несанкционированный доступ представляет собой второй способ реализации УБИ.

Уязвимые по отношению к НСД звенья представляют собой объекты среды информации на различных уровнях иерархии информационной инфраструктуры. Реализация угроз НСД осуществляется путём воздействия нарушителей на объекты среды информации с целью нарушения значимых характеристик ИБ системы.

Уязвимые по отношению к НСД звенья информационной системы представлены в таблице 4.

Таблица 4 – Уязвимые по отношению к НСД звенья информационной системы

Уровень иерархии информационной инфраструктуры	Типы объектов среды (уязвимые звенья)
Физический уровень	Линии связи внутри КЗ, линии связи вне контролируемой зоны, физические носители информации, включая НЖМД АРМ пользователей информационной системы
Сетевой уровень	Сетевое оборудование: маршрутизаторы, коммутаторы, межсетевые экраны, отделяющие информационную систему от сетей связи общего пользования
Уровень сетевых сервисов	Сетевые компоненты в составе информационной системы, сервисы терминального доступа, сервисы удалённого управления, другие служебные сервисы
Уровень ОС	Компоненты ОС, файлы, содержащие защищаемую информацию, в т.ч. ПДн
Уровень приложений	Прикладное ПО для доступа и обработки информации, в т.ч. ПДн

3.2 Возможные угрозы безопасности персональных данных

3.2.1 Угрозы утечки информации по техническим каналам

В общем, при обработке информации возможно возникновение следующих угроз утечки информации по ТКУИ:

угроза утечки акустической (речевой) информации;

угроза утечки видовой информации;

угроза утечки информации по каналам ПЭМИН.

Угроза утечки акустической информации возможна только в том случае, если в информационной системе предусмотрен голосовой ввод информации, в т.ч. ПДн, или предусмотрены функции воспроизведения информации, в т.ч. ПДн, акустическими средствами информационной системы.

На АРМ оператора ЕИС ПГиМУ СО функции голосового ввода информации или функции воспроизведения информации акустическими средствами отсутствуют.

Таким образом, реализация угрозы утечки акустической информации невозможна ввиду отсутствия источника угрозы.

Угрозы утечки видовой информации реализуются за счёт несанкционированного просмотра информации, в т.ч. ПДн, с экранов дисплеев и других средств отображения вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав информационной системы.

Экраны дисплеев рабочих мест пользователей расположены так, что визуальный просмотр информации исключен.

Таким образом, реализация угрозы утечки видовой информации признается маловероятной, а сама угроза считается неактуальной и далее не подлежит рассмотрению.

Для перехвата информации по каналам ПЭМИН нарушитель должен обладать дорогостоящей аппаратурой и иметь в своём составе специалистов высокой квалификации, достаточной для настройки аппаратуры, перехвата и выделения информативного сигнала. Кроме того, элементы АРМ оператора ЕИС ПГиМУ СО экранируются несколькими несущими стенами, и информационный сигнал маскируется множеством паразитных сигналов элементов, не входящих в информационную систему.

Эти факторы позволяют сделать вывод, что вероятность наличия возможностей осуществить перехват ПЭМИН у кого-либо из нарушителей ИБ ничтожна мала.

Таким образом, реализация угрозы утечки по каналам ПЭМИН является маловероятной, а сама угроза считается неактуальной и далее не рассматривается.

3.2.2 Угрозы несанкционированного доступа к информации

Перечень возможных угроз НСД к информации на АРМ оператора ЕИС ПГиМУ СО, факторов, приводящих к их возникновению и нарушаемых характеристик безопасности информации, обрабатываемой на АРМ оператора ЕИС ПГиМУ СО, представлен в таблице 5.

Таблица 5 – Перечень возможных угроз безопасности информации в ИС

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
Угрозы уничтожения, хищения аппаратных средств информационной системы, носителей информации путём физического доступа к элементам информационной системы		
Кража СВТ	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы системы	Конфиденциальность
Кража носителей информации	Угроза осуществляется путём НСД внешними и внутренними нарушителями к носителям информации	Конфиденциальность
Кража ключей и атрибутов доступа	Угроза осуществляется путём НСД внешними и внутренними нарушителями к носителям информации	Конфиденциальность
Кража, модификация, уничтожение информации	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИС и средства защиты, а также происходит работа пользователей	Конфиденциальность, Целостность Доступность
Вывод из строя узлов СВТ, каналов связи	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИС и проходят каналы связи	Доступность
Несанкционированное отключение встроенных средств защиты	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИС	Конфиденциальность Целостность Доступность
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
Действия вредоносных программ (вирусов)	Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций: -скрывать признаки своего присутствия в программной среде компьютера; - обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти; разрушать (искажать произвольным образом) код программ в оперативной памяти; -выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме её выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.); -сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удалённых);	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	-искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных	
Недекларированные возможности системного и прикладного ПО	Недекларированные возможности – функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации	Конфиденциальность Целостность Доступность
Установка ПО, не связанного с исполнением служебных обязанностей	Угроза осуществляется путём несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей системы или её элементов	Конфиденциальность Целостность Доступность
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и СЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
Утрата ключей и атрибутов доступа	Угроза осуществляется за счёт действия человеческого фактора пользователей ИС, которые нарушают положения парольной политики в части их создания (создают лёгкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них	Конфиденциальность Целостность Доступность
Непреднамеренная модификация (уничтожение) информации сотрудниками	Угроза осуществляется за счёт действия человеческого фактора пользователей ИС, которые нарушают положения принятых правил работы с ИС или не осведомлены о них	Целостность
Непреднамеренное отключение средств защиты	Угроза осуществляется за счёт действия человеческого фактора пользователей ИС, которые нарушают положения принятых правил работы с ИС и средствами защиты или не осведомлены о них	Конфиденциальность Целостность Доступность
Выход из строя аппаратно-программных средств	Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации	Целостность Доступность
Сбой системы электроснабжения	Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации	Целостность Доступность
Стихийное бедствие	Угроза осуществляется вследствие несоблюдения мер пожарной безопасности	
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Угроза осуществляется путём НСД внутренних нарушителей в помещения, где расположены элементы ИС и средства защиты, а также происходит работа пользователей	Конфиденциальность Целостность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Угроза осуществляется за счёт действия человеческого фактора пользователей ИС, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них	Конфиденциальность
Угрозы несанкционированного доступа по каналам связи		
«Анализ сетевого трафика»: - перехват за пределами контролируемой зоны; - перехват в пределах контролируемой зоны внешними нарушителями; - перехват в пределах контролируемой зоны внутренними нарушителями.	Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль	Конфиденциальность Целостность Доступность
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИС и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.	Конфиденциальность Целостность Доступность
Угрозы выявления паролей	Цель реализации угрозы состоит в получении НСД путём преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IPspoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путём последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.	Конфиденциальность Целостность Доступность
Угрозы получения НСД путём подмены доверенного объекта сети	Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к сети. Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения. Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.	
Угрозы типа «Отказ в обслуживании»	Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты. Могут быть выделены несколько разновидностей таких угроз: - скрытый отказ в обслуживании, вызванный привлечением части ресурсов системы на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP- соединений (SYN-flooding), шторм запросов к FTP-серверу; - явный отказ в обслуживании, вызванный исчерпанием ресурсов ИС при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam); - явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами системы при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, DNSflooding) или идентификационной и аутентификационной информации; - явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена. Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удалённого доступа к информации в системе, передача с одного адреса такого количества запросов на подключение к	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	техническому средству в составе системы, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечёт за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка системы из-за невозможности системы заниматься ничем другим, кроме обработки запросов.	
Угроза удалённого запуска приложений	Угроза заключается в стремлении запустить на хосте системы различные предварительно внедрённые вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль над работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др. Выделяют три подкласса данных угроз: - распространение файлов, содержащих несанкционированный исполняемый код; - удалённый запуск приложения путём переполнения буфера приложений серверов; -удалённый запуск приложения путём использования возможностей удалённого управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.	Конфиденциальность Целостность Доступность
Угрозы внедрения по сети вредоносных программ	К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.	Конфиденциальность Целостность Доступность

3.4 Определение актуальных угроз безопасности персональных данных

Процесс выделения актуальных угроз из общего перечня угроз выполняется в соответствии с Методикой определения актуальных угроз ФСТЭК России.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность для защищаемой информации, в т.ч. ПДн. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищённости и частота (вероятность) реализации рассматриваемой угрозы. Степень опасности каждой угрозы оценивается экспертным методом.

3.4.1 Определение уровня исходной защищённости ИС

Под уровнем исходной защищённости информационной системы понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик. Для определения уровня исходной защищённости производится оценка этих характеристик по трём качественным показателям: «Высокий», «Средний» и «Низкий».

В соответствии с Методикой определения актуальных угроз, информационной системе присваивается высокий уровень исходной защищённости, если не менее 70% характеристик соответствуют уровню «Высокий», а остальные – уровню «Средний». «Средний» уровень исходной защищённости присваивается информационной системе в случае, если не менее 70% характеристик соответствуют уровню не ниже «Средний», а остальные – «Низкому» уровню.

При составлении перечня актуальных угроз безопасности информации каждой степени исходной защищённости (Y1) ставится в соответствие числовой коэффициент, а именно:

0 - для высокой степени исходной защищённости;

5 - для средней степени исходной защищённости;

10 - для низкой степени исходной защищённости.

Результаты определения показателей исходной защищённости для АРМ оператора ЕИС ПГиМУ СО приведены в таблице 6.

Таблица 6 – Показатели исходной защищённости АРМ оператора ЕИС ПГиМУ СО

Технические и эксплуатационные характеристики ИСПДн	Уровень защищённости		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная ИСПДн, развёрнутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, сортировка, модификация, передача	-	-	+
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определённые перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	-	+	-
5. По наличию соединений с другими базами иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	-	-	+
6. По уровню обезличивания ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	-	-	+
7. По объёму ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации	+	-	-

Уровень «высокий» имеют 29% характеристик информационной системы, что меньше значения 70%. Уровень «не ниже средний» имеют 57% характеристик системы, что меньше значения 70%. Таким образом, исходная защищённость АРМ оператора ЕИС ПГиМУ СО определяется как низкая и числовой коэффициент Y1 устанавливается равным десяти (Y1 = 10).

3.3.2 Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы понимается определяемый экспертным путём показатель, характеризующий насколько вероятным является реализация конкретной УБИ в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по четырём вербальным градациям этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (Y2 = 2);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны (Y2 = 5);

высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности информации не приняты (Y2 = 10).

Оценка вероятности реализации угроз безопасности персональных данных в ИС приведена ниже.

3.3.2.1 Угрозы несанкционированного доступа к информации

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

нарушению конфиденциальности (копирование, неправомерное распространение);

нарушению целостности (уничтожение, изменение);

нарушению доступности (блокирование).

3.3.2.1.1 Угрозы уничтожения, хищения аппаратных средств информационной системы, носителей информации путём физического доступа к элементам информационной системы

Кража СВТ.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Кража носителей информации.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Кража ключей и атрибутов доступа.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Кражи, модификации, уничтожения информации.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Вывод из строя СВТ, каналов связи.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Несанкционированное отключение встроенных средств защиты.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок. Доступ к настройкам встроенных средств защиты информации предоставляется только администратору безопасности информации.

Вероятность реализации угрозы – маловероятно.

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

Действия вредоносных программ (вирусов).

На АРМ оператора ЕИС ПГиМУ СО сертифицированные ФСТЭК России средства антивирусной защиты не установлены.

Вероятность реализации угрозы – высокая.

Недекларированные возможности системного и прикладного ПО.

К использованию на АРМ оператора ЕИС ПГиМУ СО допускается только лицензионное программное обеспечение. Получение обновлений программного обеспечения осуществляется из доверенных источников.

Вероятность реализации угрозы – низкая.

Установка ПО, не связанного с исполнением служебных обязанностей.

В системе не введено разграничение прав пользователей на установку ПО, пользователи не проинструктированы о политике установки ПО.

Вероятность реализации угрозы – средняя.

3.3.2.1.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и СЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера

Утрата ключей и атрибутов доступа.

На АРМ оператора ЕИС ПГиМУ СО не введено ограничение прав пользователей на смену паролей, пользователи не проинструктированы о парольной политике.

Вероятность реализации угрозы – высокая.

Непреднамеренная модификация (уничтожение) информации сотрудниками.

Все пользователи проходят обязательный инструктаж о правилах работы на АРМ оператора ЕИС ПГиМУ СО (ознакомление с правилами работы различных приложений, необходимых для функционирования системы).

Вероятность реализации угрозы – низкая.

Непреднамеренное отключение средств защиты.

В Учреждении введён контроль доступа в контролируемую зону, все пользователи проходят обязательный инструктаж о правилах работы на АРМ оператора ЕИС ПГиМУ СО.

Вероятность реализации угрозы – маловероятно.

Сбой системы электроснабжения.

К ключевым элементам АРМ оператора ЕИС ПГиМУ СО источники бесперебойного питания не подключены.

Вероятность реализации угрозы – низкая.

Стихийное бедствие.

АРМ оператора ЕИС ПГиМУ СО расположено в помещении, оснащённом средствами пожаротушения, пользователи проинструктированы о действиях в случае возникновения нештатных ситуаций.

Вероятность реализации угрозы – маловероятно.

3.3.2.1.4 Угрозы преднамеренных действий внутренних нарушителей

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

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке.

Пользователи АРМ оператора ЕИС ПГиМУ СО осведомлены о порядке работы с защищаемой информацией, а также подписали соглашение о неразглашении.

Вероятность реализации угрозы – низкая.

3.3.2.1.5 Угрозы несанкционированного доступа по каналам связи

Угроза «Анализ сетевого трафика».

Угроза подразделяется на следующие виды:

Перехват за пределами контролируемой зоны.

На АРМ оператора ЕИС ПГиМУ СО установлены сертифицированные средства криптографической защиты типаViPNet Client 3.2.

Вероятность реализации угрозы – низкая.

Перехват в пределах контролируемой зоны внешними нарушителями.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами АРМ оператора ЕИС ПГиМУ СО оборудовано крепкими дверьми, в нерабочее время двери помещений закрываются на замок.

Вероятность реализации угрозы – маловероятно.

Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.

На АРМ оператора ЕИС ПГиМУ СО сертифицированные средства межсетевого экранирования не установлены.

Вероятность реализации угрозы – высокая.

Угроза выявления паролей.

На АРМ оператора ЕИС ПГиМУ СО сертифицированные средства межсетевого экранирования не установлены.

Вероятность реализации угрозы – высокая.

Угрозы получения НСД путём подмены доверенного объекта.

На АРМ оператора ЕИС ПГиМУ СО сертифицированные средства межсетевого экранирования не установлены.

Вероятность реализации угрозы – высокая.

Угрозы типа «Отказ в обслуживании».

На АРМ оператора ЕИС ПГиМУ СО сертифицированные средства межсетевого экранирования не установлены.

Вероятность реализации угрозы – высокая.

Угрозы удалённого запуска приложений.

На АРМ оператора ЕИС ПГиМУ СО сертифицированные средства межсетевого экранирования не установлены.

Вероятность реализации угрозы – высокая.

Угрозы внедрения по сети вредоносных программ.

На АРМ оператора ЕИС ПГиМУ СО средства межсетевого экранирования и антивирусной защиты, сертифицированные ФСТЭК России, не установлены.

Вероятность реализации угрозы – высокая.

3.3.2.2 Реализуемость угроз безопасности персональных данных

По итогам оценки уровня защищённости (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

Оценка реализуемости угроз представлена в таблице 7.

Таблица 7 - Реализуемость угроз безопасности персональных данных

Тип угроз безопасности информации	Коэффициент реализуемости угрозы (Y)	Возможность реализации
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств информационной системы путём физического доступа к элементам информационной системы		
Кража ПЭВМ	0,5	средняя
Кража носителей информации	0,5	средняя
Кража ключей и атрибутов доступа	0,5	средняя
Кражи, модификации, уничтожение информации	0,5	средняя
Вывод из строя СВТ, каналов связи	0,5	средняя
Несанкционированное отключение средств защиты	0,5	средняя
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
Действия вредоносных программ (вирусов)	1	очень высокая
Недекларированные возможности системного и прикладного ПО	0,6	средняя
Установка ПО, не связанного с исполнением служебных обязанностей	0,75	высокая
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и СЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
Утрата ключей и атрибутов доступа	1	очень высокая
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,6	средняя
Непреднамеренное отключение средств защиты	0,5	средняя
Сбой системы электроснабжения	0,6	средняя
Стихийное бедствие	0,5	средняя
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенных к её обработке	0,5	средняя
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	0,6	средняя
Угрозы несанкционированного доступа по каналам связи.		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из информационной системы и принимаемой из внешних сетей информации:		
Перехват за переделами контролируемой зоны	0,6	средняя
Перехват в пределах контролируемой зоны внешними нарушителями	0,5	средняя
Перехват в пределах контролируемой зоны внутренними нарушителями	0,5	средняя
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	1	очень высокая
Угрозы выявления паролей	1	очень высокая
Угроза получения НСД путём подмены доверенного объекта	1	очень высокая
Угрозы типа «Отказ в обслуживании»	1	очень высокая
Угрозы удалённого запуска приложений	1	очень высокая
Угрозы внедрения по сети вредоносных программ	1	очень высокая

3.3.2.3 Определение опасности и актуальности угроз безопасности информации

При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определялся вербальный показатель опасности для узла информационной системы. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из перечня угроз безопасности тех, которые относятся к актуальным для данной информационной системы, в соответствии с правилами, представленными в таблице 8.

Таблица 8 – Правила отнесения угрозы безопасности к актуальной

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

Результаты оценки актуальности угроз для АРМ оператора ЕИС ПГиМУ СО приведены в таблице 9.

Таблица 9 - Актуальные угрозы безопасности информации

Тип угроз	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы несанкционированного доступа к информации			
Угрозы уничтожения, хищения аппаратных средств информационной системы путем физического доступа к элементам информационной системы			
Кража СВТ	средняя	низкая	неактуальная
Кража носителей информации	средняя	низкая	неактуальная
Кража ключей и атрибутов доступа	средняя	низкая	неактуальная
Кражи, модификации, уничтожения информации	средняя	низкая	неактуальная
Вывод из строя СВТ, каналов связи	средняя	низкая	неактуальная
Несанкционированное отключение средств защиты	средняя	низкая	неактуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)			
Действия вредоносных программ (вирусов)	очень высокая	средняя	актуальная
Недекларированные возможности системного и прикладного ПО	средняя	низкая	неактуальная
Установка ПО, не связанного с исполнением служебных обязанностей	высокая	средняя	актуальная

Тип угроз	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и СЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера			
Утрата ключей и атрибутов доступа	очень высокая	средняя	актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя	средняя	актуальная
Непреднамеренное отключение средств защиты	средняя	средняя	актуальная
Сбой системы электроснабжения	средняя	низкая	неактуальная
Стихийное бедствие	средняя	низкая	неактуальная
Угрозы преднамеренных действий внутренних нарушителей			
Доступ к информации, модификация, уничтожение лицами, не допущенными к её обработке	средняя	средняя	актуальная
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	средняя	средняя	актуальная
Угрозы несанкционированного доступа по каналам связи			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:			
Перехват за переделами контролируемой зоны	средняя	средняя	актуальная
Перехват в пределах контролируемой зоны внешними нарушителями	средняя	низкая	неактуальная
Перехват в пределах контролируемой зоны внутренними нарушителями	средняя	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	очень высокая	средняя	актуальная
Угрозы выявления паролей	очень высокая	средняя	актуальная
Угроза получения НСД путём подмены доверенного объекта	очень высокая	средняя	актуальная
Угрозы типа «Отказ в обслуживании»	очень высокая	низкая	актуальная
Угрозы удалённого запуска приложений	очень высокая	средняя	актуальная
Угрозы внедрения по сети вредоносных программ	очень высокая	средняя	актуальная

Таким образом, в результате анализа были выявлены следующие актуальные угрозы:
действия вредоносных программ (вирусов);
установка ПО, не связанного с исполнением служебных обязанностей;
утрата ключей и атрибутов доступа;
непреднамеренная модификация (уничтожение) информации сотрудниками;
непреднамеренное отключение средств защиты;

доступ к информации, модификация, уничтожение лицами, не допущенными к её обработке;

разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке;

перехват за переделами контролируемой зоны;

угрозы сканирования, направленные на выявление типа операционной системы элементов ИС, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей;

угроза получения НСД путём подмены доверенного объекта;

угрозы типа «Отказ в обслуживании»;

угрозы удалённого запуска приложений;

угрозы внедрения по сети вредоносных программ.

4 ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДн

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» АРМ оператора ЕИС ПГиМУ СО относится к информационным системам, обрабатывающим иные категории персональных данных субъектов ПДн, являющихся сотрудниками оператора и менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для АРМ оператора ЕИС ПГиМУ СО, актуальны угрозы безопасности информации, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для АРМ оператора ЕИС ПГиМУ СО актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об АРМ оператора ЕИС ПГиМУ СО, на основе анализа угроз безопасности информации, и в соответствии с п.п. 8-12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» на АРМ оператора ЕИС ПГиМУ СО, необходимо обеспечить 4-й уровень защищенности ПДн.

5 СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

5.1 Базовый набор мер по защите информации

Учитывая, что меры по обеспечению безопасности персональных данных и порядок их выбора, установленные Составом и содержанием мер, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21, аналогичны мерам защиты информации и порядку их выбора, установленным Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, для обеспечения защиты информации, обрабатываемой на АРМ оператора ЕИС ПГиМУ СОв дальнейшем будем руководствоваться только Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Вместе с тем для обеспечения безопасности персональных данных при их обработке на АРМ оператора ЕИС ПГиМУ СОв дополнение к Требованиям, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17, необходимо руководствоваться требованиями (в том числе в части определения уровня защищенности персональных данных), установленными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. При этом в соответствии с пунктом 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, должно быть обеспечено соответствующее соотношение класса защищенности информационной системы с уровнем защищенности персональных данных. В случае, если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение пункта 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Выбор мер защиты информации осуществляется исходя из класса защищенности АРМ оператора ЕИС ПГиМУ СО, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности информации, включенных в модель угроз, а также с учетом структурно-функциональных характеристик АРМ оператора ЕИС ПГиМУ СО, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации, а также иные характеристики системы, применяемые информационные технологии и особенности функционирования.

Таблица 10 - Базовый набор мер по защите информации данных для обеспечения класса защищенности К4

Условное обозначение и номер меры	Меры защиты информации в информационной системе
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	

Условное обозначение и номер меры	Меры защиты информации в информационной системе
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между информационными системами
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	информационной системе
РСБ. 7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

5.2 Адаптация базового набора мер по защите информации

С учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с

информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе, для АРМ оператора ЕИС ПГиМУ СО необходимо принятие адаптированного набора мер защиты информации, приведенного в таблице 11.

Таблица 11 – Адаптированный набор мер по обеспечению безопасности персональных данных

Условное обозначение и номер меры	Меры защиты информации в информационной системе
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между информационными системами
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	

Условное обозначение и номер меры	Меры защиты информации в информационной системе
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ. 7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

5.3 Уточнение адаптированного базового набора мер по защите информации

Уточнение адаптированного базового набора мер по защите информации проводится с учетом результатов оценки возможности адаптированного базового набора мер по защите информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности ПДн, или снизить вероятность их реализации исходя из условий функционирования информационной системы.

Исходными данными при уточнении адаптированного базового набора мер по обеспечению защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз.

Состав и содержание уточненного адаптированного базового набора мер по обеспечению защиты информации на АРМ оператора ЕИС ПГиМУ СО приведены в таблице 12.

Таблица 12 – Уточненный адаптированный набор мер по защите информации

Условное обозначение и номер меры	Меры защиты информации в информационной системе
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

Условное обозначение и номер меры	Меры защиты информации в информационной системе
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ. 7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

5.4 Дополнение уточненного адаптированного базового набора мер защиты информации

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10.07.2014 г. № 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» для обеспечения 4–го уровня защищенности ПДн при их обработке на АРМ оператора ЕИС ПГиМУ СО необходимо выполнение следующих требований:

назначение ответственного за обеспечение функционирования и безопасности криптосредств;

обучение лиц, использующих криптосредства, работе с ними;

организация поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним;

организация учета лиц, допущенных к работе с СКЗИ, предназначенных для обеспечения безопасности ПДн в ИСПДн;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, в т.ч. оснащение помещений входными дверями с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

утверждение правил доступа в помещения, в которых размещена информационная система, в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждения перечня лиц, имеющих право доступа в помещения, в которых размещена информационная система;

использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

организация учета машинных носителей информации (персональных данных);

организация хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6 РЕКОМЕНДУЕМЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Для выполнения требований Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных», приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и для обеспечения 3-го уровня защищенности персональных данных в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» рекомендуется осуществить мероприятия по физической и программно-аппаратной защите, а так же ряд мероприятий организационного характера.

Рекомендации по проведению мероприятий по обеспечению безопасности персональных данных при их обработке на АРМ оператора ЕИС ПГиМУ СО приведены в таблице 13.

Таблица 13 – Мероприятия по обеспечению защиты информации на АРМ оператора ЕИС ПГиМУ СО

Условное обозначение и номер меры	Содержание мер защиты информации	Мероприятия по обеспечению защиты информации	
		Технические	Организационные
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Использование сертифицированных ФСТЭК России СЗИ от НСД	
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей системы
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей системы
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Отображение символа «*» или «•» при вводе аутентификационной информации	
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж администраторов информационной системы
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка матрицы доступа субъектов доступа к объектам доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России	

Условное обозначение и номер меры	Содержание мер защиты информации	Мероприятия по обеспечению защиты информации	
		Технические	Организационные
	информационными системами		
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, матрицы доступа
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж пользователей системы
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		Разработка инструкций, инструктаж пользователей системы
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Использование сертифицированных средств межсетевого экранирования	
III. Ограничение программной среды			
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		Разработка инструкций, инструктаж пользователей системы
IV. Защита машинных носителей информации			
ЗНИ.1	Учет машинных носителей информации		Разработка инструкций, инструктаж пользователей системы
ЗНИ.2	Управление доступом к машинным носителям информации		Разработка инструкций, инструктаж пользователей системы
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж пользователей системы
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля	Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля	Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств	

Условное обозначение и номер меры	Содержание мер защиты информации	Мероприятия по обеспечению защиты информации	
		Технические	Организационные
		межсетевого экранирования, средств антивирусного контроля	
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти		Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Штатные средства ОС	
РСБ. 7	Защита информации о событиях безопасности	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля	
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Использование средств антивирусной защиты, сертифицированных ФСТЭК России	Разработка инструкции по организации антивирусной защиты, проведение инструктажа пользователей
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Использование средств антивирусной защиты, сертифицированных ФСТЭК России	Инструктаж пользователей и администраторов системы
VII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		Разработка инструкций, инструктаж пользователей и администраторов информационной системы
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		Разработка организационно-распорядительной документации, регламентирующей проведение периодического контроля ИС, в т.ч. состава технических средств, программного обеспечения и средств защиты информации

Условное обозначение и номер меры	Содержание мер защиты информации	Мероприятия по обеспечению защиты информации	
		Технические	Организационные
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения средств защиты информации	Использование сертифицированных ФСТЭК России СЗИ от НСД	
XII. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования		Утверждение схемы границ контролируемой зоны информационной системы
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены		Разработка организационно-распорядительной документации, обеспечивающей ограничение доступа посторонних лиц в пределах КЗ, ограничение доступа к средствам защиты информации, к техническим средства и средствам обеспечения функционирования информационной системы
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		Разработка инструкций, проведение инструктажа пользователей информационной системы, ограничение доступа посторонних лиц в пределы КЗ
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны	Использование СКЗИ, сертифицированных ФСБ России	Разработка инструкций, инструктаж пользователей
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	Использование средств межсетевого экранирования, сертифицированных ФСТЭК России	
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	Использование средств межсетевого экранирования, сертифицированных ФСТЭК России	

6.1 Организационные мероприятия

В рамках СЗИ рекомендуется реализовать следующие организационные меры защиты:

назначить должностное лицо (работка), ответственное за защиту информации в информационной системе;

назначить сотрудника, ответственного за обеспечение функционирования и безопасности криптосредств;

разработать документы, регламентирующие обработку защищаемой информации, в т.ч. ПДн, в информационной системе;

организовать разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке информации и иных функций;

организовать процедуры доступа работников в помещение с элементами информационной системы, а также к техническим средствам, предназначенным для обработки информации, в т.ч. ПДн;

организовать процедуры ознакомления работников, непосредственно осуществляющих обработку информации, в т.ч. ПДн, с требованиями законодательных и нормативных актов в области защиты информации;

организовать инструктаж лиц, использующих средства защиты информации, применяемые в информационной системе, правилам работы с ними;

организовать процедуры контроля за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

организовать процедуры учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;

установить правила разграничения доступа к информационным ресурсам информационной системы;

организовать правила антивирусной защиты информации;

организовать учет лиц, допущенных к работе в информационной системе;

организовать учет машинных носителей информации;

организовать процедуры резервного копирования;

организовать правила парольной защиты;

организовать поэкземплярный учет криптосредств, эксплуатационной и технической документации к ним;

организовать учет лиц, допущенных к работе с СКЗИ, предназначенными для защиты информации, в т.ч. ПДн, в информационной системе;

организовать процедуры периодического внутреннего контроля и (или) аудита соответствия обработки информации требованиям законодательных и нормативных актов в области защиты информации.

6.2 Мероприятия по физической защите

Применяемые технические меры защиты информации должны обеспечивать защиту от несанкционированного доступа к информации.

Должна быть организована охрана помещений, в которых размещены элементы АРМ оператора ЕИС ПГиМУ СО и производится обработка персональных данных. Организация режима обеспечения безопасности этих помещений должна обеспечивать сохранность носителей информации и средств защиты информации, и исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения с элементами АРМ оператора ЕИС ПГиМУ СО должны быть оснащены крепкими дверьми с замками и приспособлениями для опечатывания, или

соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

6.3 Методы и способы защиты информации от несанкционированного доступа

Для защиты от несанкционированного доступа к информации, рекомендуется применение следующих методов и способов:

организация физической защиты помещений и технических средств информационной системы;

размещение технических средств, предназначенных для обработки защищаемой информации, в пределах контролируемой зоны;

ограничение доступа пользователей в помещения, где размещены технические средства информационной системы, а также хранятся носители информации;

установление правил доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

управление доступом к защищаемой информации;

регистрация и учет действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

использование защищенных каналов связи;

использование средств межсетевого экранирования;

применение средств антивирусной защиты информации;

применение средств криптографической защиты информации.

Обеспечение защиты информации на АРМ оператора ЕИС ПГиМУ СО должно быть реализовано средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия.

ЗАКЛЮЧЕНИЕ

На основании представленной в модели нарушителя совокупности предположений о возможностях, которые могут использоваться при создании шаблонов, подготовке и проведении атак, а также с учетом 3-го типа актуальных угроз, уровень криптографической защиты информации, обеспечиваемый криптосредствами в информационной системе, должен соответствовать уровню не ниже КС1 (в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности), при условии соблюдения организационно-режимных и кадрово-режимных мер, действующих в отношении пользователей и на местах эксплуатации криптосредств.

Построение настоящей модели позволило определить актуальные угрозы безопасности информации (Таблица 9).

Для обеспечения требований законодательства Российской Федерации, методических и руководящих документов органов государственной власти для АРМ оператора ЕИС ПГиМУ СО должны быть реализованы меры по противодействию актуальным угрозам безопасности информации. Используемые при этом средства защиты информации должны обладать действующими сертификатами соответствия устанавливаемым к данным средствам защиты информации требованиями ФСТЭК России и/или ФСБ России.