Утверждена
приказом ГБУЗ РТ «Сут-Хольская ЦКБ»
от «05» марта 2020 г. № 95

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**ГБУЗ РТ «СУТ-ХОЛЬСКАЯ ЦКБ»**

Обозначения и сокращения

**АВС** - антивирусные средства;

**АРМ** - автоматизированное рабочее место;

**ВТСС** - вспомогательные технические средства и системы;

**ИСПДн** - информационная система персональных данных;

**КЗ** - контролируемая зона;

**ЛВС** - локальная вычислительная сеть;

**МЭ** - межсетевой экран;

**НСД** - несанкционированный доступ;

**ОС** - операционная система;

**ПДн** - персональные данные;

**ПМВ** - программно-математическое воздействие;

**ПО** - программное обеспечение;

**ПЭМИН**-побочные электромагнитные излучения и наводки;

**САЗ -** система анализа защищенности;

**СЗИ** - средства защиты информации;

**СЗПДн** - система (подсистема) защиты персональных данных;

**СОВ** - система обнаружения вторжений;

**ТКУИ** - технические каналы утечки информации;

**УБПДн** - угрозы безопасности персональных данных;

**ФСТЭК России** - Федеральная служба по техническому и экспортному контролю.

 **Определения** В настоящем документе используются следующие термины и их определения:
автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную выполнения установленных функций;

 блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

 вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных;
 доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ;
 закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);
 информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
 контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

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

нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действие, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;

неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

 несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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, применяемые в информационных системах;
 перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

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

программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;

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;

утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;
 уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**1. Общие положения**

Настоящая Модель определяет актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее - информационная система) в ГБУЗ РТ «Сут-Хольская ЦКБ».

Настоящая Модель угроз разработана в соответствии со следующими основными документами:

[Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051);

[Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046);

[Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных](http://docs.cntd.ru/document/902072133), утвержденным [постановлением Правительства Российской Федерации от 17 ноября 2007 года N 781](http://docs.cntd.ru/document/902072133) (далее - Положение);

[Порядком проведения классификации информационных систем персональных данных](http://docs.cntd.ru/document/902094696), утвержденным [приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года N 55/86/20](http://docs.cntd.ru/document/902094696) (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный N 11462) (далее - Порядок);

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.);

Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.).

В соответствии с п. 2 Положения безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

В соответствии с п. 12 Положения необходимым условием разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных (далее - модель угроз).

Кроме этого, в соответствии с п. 16 Порядка модель угроз необходима для определения класса специальной информационной системы.

Модель угроз формируется и утверждается оператором <1> в соответствии с методическими документами, разработанными в соответствии с пунктом 2 [постановления Правительства Российской Федерации от 17 ноября 2007 года N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"](http://docs.cntd.ru/document/902072133).

Модель угроз может быть пересмотрена:

по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<1> оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместное другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**2. Описание ИСПДн**

Описание ИСПДн является первым шагом при построении модели угроз и осуществляется на этапе сбора и анализа исходных данных.

Описание ИСПДн состоит из следующих пунктов:

1) описание условий создания и использования ПДн;

описание форм представления ПДн;

описание структуры ИСПДн;

описание характеристик безопасности.

**2.1. Определение характеристик безопасности**

 Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

 Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

 Доступность информации - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

 При обработке персональных данных в ИСПДн МЗ РТ необходимо обеспечить следующие характеристики безопасности - конфиденциальность, целостность.

**3. Пользователи ИСПДн Сут-Хольская ЦКБ**

Основные группы пользователей ИСПДн:

администратор ИСПДн, осуществляющий настройку и установку технических средств ИСПДн и обеспечивающий ее бесперебойную работу;

операторы ИСПДн, осуществляющие текущую работу с персональными данными. Матрица доступа для ИСПДн МЗ РТ представлена в таблице 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Роль | Уровень доступа к ПДн | Разрешенные действия |
| Администратор ИСПДн | обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;обладает полной информацией о технических средствах и конфигурации ИСПДн;имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;обладает правами конфигурирования и административной настройки технических средств ИСПДн | - сбор;- систематизация;- накопление;- хранение;- уточнение;- использование;- распространение;- обезличивание;- блокирование;- уничтожение |
| Оператор ИСПДн | обладает правами доступа к подмножеству ПДн;Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационных систем, через которые он осуществляет доступ, и о составе технических средств ИСПДн | - сбор;- систематизация;- накопление;- хранение;- уточнение;- использование;- распространение;- обезличивание |

**4. Описание угроз в ГБУЗ РТ «Сут-Хольская ЦКБ»**

**4.1. Модель нарушителя**

 Источниками угроз НСД в ИС могут быть:

нарушитель;
носитель вредоносной программы;

аппаратная закладка.

По признаку принадлежности все нарушители делятся на две группы:

- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой находится ИС, в которой циркулирует информация;
- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой находится ИС, в которой циркулирует информация.
Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядок проведения работ, направленных на предотвращение и пресечение несанкционированных действий. Исходя из особенностей функционирования ИС допущенные к ней физические лица имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИС в соответствии с принятой политикой информационной безопасности. К внутренним нарушителям могут относиться:
- администраторы ИС;

- пользователи ИС;

- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИС, но не имеющие права доступа к ресурсам;

- обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.).

В зависимости от квалификации нарушителей рассматриваются следующие категории:
1) хакер-одиночка;

2) объединенная хакерская группа;

3) предприятие-конкурент.

Классификация нарушителей по мотивации:

- хакеры-одиночки;

- промышленные шпионы;

- профессиональные преступники.

Среди целей, преследуемых нарушителями, отмечаются:

- любопытство;

- вандализм;

- месть;

- финансовая выгода;

- конкурентная выгода;

- сбор информации.

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

К внешним нарушителям могут относиться:

- бывшие сотрудники - администраторы или пользователи ИС;

- посторонние лица, пытающиеся получить доступ к информации в инициативном порядке.

**4.2. Угрозы безопасности информации ГБУЗ РТ «Сут-Хольская ЦКБ»**

Исходный класс защищенности - средний.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе |
|  |  |  |  |  | технические | организационные |
| 1. Угрозы от утечки по техническим каналам |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 1.1. Угрозы утечки видовой информации | маловероятно | низкая | низкая | неактуальная | жалюзи на окна | пропускной режим |
|  |  |  |  |  |  | инструкция пользователя |
| 1.2. Угрозы утечки информации по каналам ПЭМИН | маловероятно | низкая | низкая | неактуальная | генераторы пространственного зашумления | технологический процесс обработки |
|  |  |  |  |  | генератор шума по цепи электропитания | контур заземления |
| 2. Угрозы несанкционированного доступа к информации |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн: |
| 2.1.1. кража ПЭВМ | маловероятно | низкая | низкая | неактуальная | решетки на окна | акт установки средств защиты |
|  |  |  |  |  | металлическая дверь |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  | шифрование данных |  |
| 2.1.2. кража носителей информации | маловероятно | низкая | низкая | неактуальная | шифрование данных | учет носителей информации |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 2.1.3. кража ключей доступа | маловероятно | низкая | низкая | неактуальная | хранение в сейфе | инструкция пользователя |
|  |  |  |  |  | решетки на окна |  |
|  |  |  |  |  | металлическая дверь |  |
|  |  |  |  |  | шифрование данных  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  | система защиты от НСД |  |
| 2.1.4. вывод из строя узлов ПЭВМ, каналов связи | маловероятно | низкая | низкая | неактуальная | решетки на окна |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  | металлическая дверь |  |
|  |  |  |  |  |  |  |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий): |
| 2.2.1. действия вредоносных программ (вирусов) | низкая | средняя | средняя | актуальная | антивирусное ПО | инструкция пользователя |
|  |  |  |  |  |  | инструкция ответственного |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | технологический процесс обработки |
|  |  |  |  |  |  | инструкция по антивирусной защите |
|  |  |  |  |  |  | акт установки средств защиты |
| 2.2.2. недекларированные возможности системного ПО и ПО для обработки персональных данных | маловероятно | низкая | низкая | неактуальная |  | сертификация |
| 2.2.3. установка ПО, не связанного с исполнением служебных обязанностей | маловероятно | низкая | низкая | неактуальная | настройка средств защиты | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
| 2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера: |
| 2.3.1. утрата ключей и атрибутов доступа | низкая | средняя | средняя | актуальная |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
| 2.3.2. непреднамеренная модификация (уничтожение) информации сотрудниками | маловероятно | низкая | низкая | неактуальная | настройка средств защиты | резервное копирование |
| 2.3.4. выход из строя аппаратно-программных средств | маловероятно | низкая | низкая | неактуальная |  | резервирование |
| 2.3.5. сбой системы электроснабжения | маловероятно | низкая | низкая | неактуальная | использование источника бесперебойного электропитания | резервное копирование |
| 2.3.6. стихийное бедствие | маловероятно | низкая | низкая | неактуальная | пожарная сигнализация |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей: |
| 2.4.1. доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | маловероятно | низкая | низкая | неактуальная | система защиты от НСД | акт установки средств защиты |
|  |  |  |  |  |  | разрешительная система допуска |
|  |  |  |  |  |  | технологический процесс обработки |
|  |  |  |  |  |  |  |
| 2.4.2. разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | низкая | средняя | низкая | неактуальная |  | договор о не разглашении |
|  |  |  |  |  |  | инструкция пользователя |
| 2.5. Угрозы несанкционированного доступа по каналам связи: |
| 2.5.1. угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: |  |  |
| 2.5.1.1. перехват за пределами контролируемой зоны | низкая | средняя | низкая | неактуальная | шифрование | технологический процесс |
| 2.5.1.2. перехват в пределах контролируемой зоны внешними нарушителями | маловероятно | низкая | низкая | неактуальная | шифрование |  |
|  |  |  |  |  | физическая защита канала связи | технологический процесс |
| 2.5.1.3. перехват в пределах контролируемой зоны внутренними нарушителями | маловероятно | низкая | низкая | неактуальная | шифрование | технологический процесс |
|  |  |  |  |  | физическая защита канала связи |  |
| 2.5.2. угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | маловероятно | низкая | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | акт установки средств защиты |
| 2.5.3. угрозы выявления паролей по сети | низкая | средняя | средняя | актуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | акт установки средств защиты |
| 2.5.4. угрозы навязывание ложного маршрута сети | маловероятно | низкая | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | акт установки средств защиты |
| 2.5.5. угрозы подмены доверенного объекта в сети | маловероятно | низкая | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
| 2.5.6. угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | маловероятно | низкая | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | акт установки средств защиты |
| 2.5.7. угрозы типа "Отказ в обслуживании" | маловероятно | низкая | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  | антивирусное ПО | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | резервирование |
| 2.5.8. угрозы удаленного запуска приложений | низкая | средняя | низкая | неактуальная | межсетевой экран | технологический процесс |
|  |  |  |  |  | антивирусное ПО | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
| 2.5.9. угрозы внедрения по сети вредоносных программ | низкая | средняя | средняя | актуальная | антивирусное ПО | технологический процесс |
|  |  |  |  |  |  | инструкция пользователя |
|  |  |  |  |  |  | инструкция администратора безопасности |
|  |  |  |  |  |  | акт установки средств защиты |

 Таким образом, актуальными угрозами безопасности ПДн в автономной ИС II типа являются:
- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;

инструкции пользователей ИСПДн, в которых отражен порядок безопасной работы с ИСПДн в сетях общего пользования и (или) международном обмене, а также с ключами и атрибутами доступа;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международному обмену (сеть "Интернет"), если это не требуется для функционирования ИСПДн.