Приложение № 2
к приказу Министерства
архитектуры и строительства
Смоленской области
от «14» 08 2025 г. №140-ОД

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ «САЙТ», С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ МИНИСТЕРСТВА АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

Смоленск
2025

Оглавление

1. Термины и определения

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура – совокупность основных структурно-функциональных характеристик, свойств, компонентов информационная система «Сайт», воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с ИС и не включена оператором системы или сети в границу процесса оценки угроз безопасности информации.

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.

Возможности нарушителя – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

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

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

Информация – данные, содержащиеся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент – программное, программно-аппаратное или техническое средство, входящее в состав ИС.

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

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

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение информации.

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и

иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

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

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

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

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

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

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

Программное обеспечение – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

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

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

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

Угроза безопасности информации (УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

2. Общие положения

2.1. Введение

2.1.1. Настоящая модель угроз безопасности информации, обрабатываемой в информационной системе с использованием средств криптографической защиты информации, (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.

2.1.2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в информационной системе «Сайт» (далее – ИС) (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в ИС информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования ИС – актуальных угроз безопасности информации.

2.1.3. В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» настоящая Модель угроз подлежит использованию при формировании требований к системе защиты ПДн, обрабатываемых в ИС.

2.2. Источники разработки

2.2.1. Настоящая Модель угроз сформирована в соответствии с методическими документами ФСТЭК России и ФСБ России с учетом следующих принципов:

– в случае обеспечения безопасности информации без использования СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России;

– в случае определения Министерством архитектуры и строительства Смоленской области (далее – Министерство) необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.

2.2.2. Перечень нормативных правовых актов, методических документов и национальных стандартов, используемый для оценки угроз безопасности информации и разработки Модели угроз:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами,

являющимися государственными или муниципальными органами»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;

– Приказ Федеральной службы безопасности Российской Федерации от 10 июля 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»;

– 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, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации 31 марта 2015 г. № 149/7/2/6-432;

– ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1520-ст;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», утвержденный постановлением Госстандарта России от 9 февраля 1995 г. № 49;

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», утвержденный постановлением Госстандарта России от 14 июля 1998 г. № 295;

– ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к

содержанию документов», утвержденный приказом Росстандарта от 25 октября 2021 г. № 1297-ст;

– Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», утвержденный Решением председателя Гостехкомиссии России от 30 марта 1992 г.

2.3. Оцениваемые угрозы

2.3.1. Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (далее – ТКУИ), по причинам, перечисленным в таблице 1.

Таблица 1 – Обоснования исключения угроз, реализуемых за счет ТКУИ

№ п/п	Угрозы, связанные с техническими каналами утечки информации	Обоснование исключения
1.	Угрозы утечки акустической (речевой) информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящую специализированную аппаратуру, регистрирующую акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки информации, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз.

№ п/п	Угрозы, связанные с техническими каналами утечки информации	Обоснование исключения
2.	Угрозы утечки видовой информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих специализированные оптические (оптико-электронные) средства для 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 системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз.
3.	Угрозы утечки информации по каналам ПЭМИН	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящие специализированные технические средства перехвата побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз.

* За исключением угроз, характеризующихся использованием нарушителями портативных (мобильных) устройств съема информации (планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

2.4. Участники функционирования системы (сети)

2.4.1. Информация об организациях, имеющих отношение к ИС, представлена в таблице 2.

Таблица 2 – Перечень организаций

№ п/п	Роль организации	Организация
1.	Оператор системы	Министерство архитектуры и строительства Смоленской области

2.5. Ответственность за обеспечение защиты информации (безопасности)

2.5.1. Ответственными за обеспечение безопасности ПДн при их обработке в ИС, приказом Министра архитектуры и строительства Смоленской области назначены должностные лица / подразделения, представленные в таблице 3.

Таблица 3 – Ответственные за обеспечение защиты информации (безопасности)

№ п/п	Роль подразделения / должностного лица	Должностное лицо / подразделение
1.	Ответственный за обеспечение безопасности персональных данных	Начальник отдела цифровизации и информационных систем (Отдел цифровизации и информационных систем)

2.6. Особенности пересмотра Модели угроз

2.6.1. Настоящая Модель угроз может быть пересмотрена:

– по решению Министерства на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений ИС;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности информации;

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИС;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в ИС и (или) взаимодействующих (смежных) системах.

3. Описание систем и сетей и их характеристика как объектов защиты

3.1. Общее описание объекта оценки угроз

3.1.1. Настоящая Модель угроз разработана в отношении ИС.

3.1.2. Основные характеристики ИС:

3.1.2.1. Состав обрабатываемой информации:

– Общедоступная информация.

3.1.2.2. Основные процессы (бизнес-процессы), для обеспечения которых создана ИС:

– Оказание государственных и муниципальных услуг (Предполагает организацию предоставления государственных и муниципальных услуг в соответствии с законодательством Российской Федерации);

– Ведение веб-ресурсов (Предполагает деятельность, связанную с наполнением официального сайта организации, предоставлением доступа пользователям к сервисам, информации и материалам на сайте, совершенствованием способов и методов представления информации на сайте, улучшением обслуживания пользователей с учетом положений законодательства).

3.1.2.3. Уровень защищенности ПДн: 4 («Акт определения уровня защищенности персональных данных при их обработке в информационная система «Сайт» Министерства архитектуры и строительства Смоленской области»).

3.2. Состав и архитектура объекта оценки

3.2.1. Состав ИС определен в таблице 4.

Таблица 4 – Состав ИС

№ п/п	Характеристика	Значение характеристики
1.	Программно-аппаратные средства	ОС-407-ZK-D09 – 1 ОС-101-ZK-D10 – 1
2.	Общесистемное программное обеспечение	- Windows 7 Профессиональная; Windows 10 Pro
3.	Прикладное программное обеспечение	- Веб-сервер Apache
4.	Средства защиты информации	**Криптографическая защита:** - «КриптоПро CSP» версия 4.0 R4 (исполнение 1-Base) (Сертифицирующий орган ФСБ России № СФ/114-4716 от 15.01.2024 действителен до 15.01.2026) **Антивирусная защита:** - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСБ России № СФ/СЗИ-0523 от 15.12.2021 действителен до 01.11.2026; Сертифицирующий

№ п/п	Характеристика	Значение характеристики
		орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029) **Контроль съемных машинных носителей информации:** - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029)

3.2.2. ИС представляет собой распределенную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в одном или нескольких субъектах РФ и объединенных в единую систему с использованием сетей электросвязи) со следующими характеристиками:

3.2.2.1. Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – имеется.

3.2.2.2. Подключение к ИТКС Министерства – отсутствует.

3.2.2.3. Подключение к ИТКС «Интернет» – имеется.

3.2.2.4. Подключение к ИТКС иных организаций – отсутствует.

3.2.2.5. В ИС не осуществляется взаимодействие с системами и сетями других организаций.

3.2.2.6. В ИС не осуществляется взаимодействие с другими системами и сетями Министерства.

3.2.2.7. К информационным ресурсам ИС не осуществляется локальный доступ.

3.2.2.8. К информационным ресурсам ИС осуществляется удаленный доступ. Особенности удаленного доступа приведены в таблице 5.

Таблица 5 – Удаленный доступ

Лица, осуществляющие удаленный доступ	Цель доступа	Способ доступа	Куда осуществляется доступ
Пользователи	информационная	с помощью подключения через браузер	Ко всем узлам системы

3.2.3. Технологии, используемые в ИС отражены в таблице 6.

Таблица 6 – Технологии, используемые в ИС

№ п/п	Технология	Используется / Не используется
1.	Съемные носители информации	Не используется
2.	Технология виртуализации	Не используется
3.	Технология беспроводного доступа	Не используется
4.	Мобильные технические средства	Не используется
5.	Веб-серверы	Используется
6.	Технология веб-доступа	Не используется
7.	Smart-карты	Не используется
8.	Технологии грид-систем	Не используется
9.	Технологии суперкомпьютерных систем	Не используется
10.	Большие данные	Не используется
11.	Числовое программное оборудование	Не используется
12.	Одноразовые пароли	Не используется
13.	Электронная почта	Не используется
14.	Технология передачи видеоинформации	Не используется
15.	Технология удаленного рабочего стола	Не используется
16.	Технология удаленного администрирования	Не используется
17.	Технология удаленного внеполосного доступа	Не используется
18.	Технология передачи речи	Не используется
19.	Технология искусственного интеллекта	Не используется

3.2.4. ИС функционирует на базе инфраструктуры Министерства архитектуры и строительства Смоленской области.

4. Актуальные угрозы безопасности информации

4.1. В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для ИС – актуальные угрозы безопасности информации.

4.2. В соответствии с методическим документом «Методика оценки угроз безопасности информации», утвержденным Федеральной службой по техническому и экспортному контролю от 5 февраля 2021 г., выявлено актуальных угроз: 125. Перечень актуальных угроз безопасности информации представлен в таблице 7.

Таблица 7 – Актуальные угрозы безопасности информации

Идентификатор угрозы	**Наименование угрозы**
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.032	Угроза использования поддельных цифровых подписей BIOS
УБИ.033	Угроза использования слабостей кодирования входных данных

Идентификатор угрозы	Наименование угрозы
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.041	Угроза межсайтового скриптинга
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.088	Угроза несанкционированного копирования защищаемой информации
УБИ.089	Угроза несанкционированного редактирования реестра
УБИ.090	Угроза несанкционированного создания учётной записи пользователя
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.093	Угроза несанкционированного управления буфером

Идентификатор угрозы	Наименование угрозы
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.103	Угроза определения типов объектов защиты
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.127	Угроза подмены действия пользователя путём обмана
УБИ.128	Угроза подмены доверенного пользователя
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.132	Угроза получения предварительной информации об объекте защиты
УБИ.139	Угроза преодоления физической защиты
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL

Идентификатор угрозы	Наименование угрозы
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.156	Угроза утраты носителей информации
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.158	Угроза форматирования носителей информации
УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.162	Угроза эксплуатации цифровой подписи программного кода
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.169	Угроза наличия механизмов разработчика
УБИ.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.172	Угроза распространения «почтовых червей»
УБИ.173	Угроза «спама» веб-сервера
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
УБИ.179	Угроза несанкционированной модификации защищаемой информации
УБИ.182	Угроза физического устаревания аппаратных компонентов
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.188	Угроза подмены программного обеспечения
УБИ.189	Угроза маскирования действий вредоносного кода
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

Идентификатор угрозы	Наименование угрозы
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза перехвата управления информационной системой
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

4.3. Перечень актуальных угроз, приведенный выше, определен без учета реализованного комплекса мероприятий организационного и технического характера, снижающего вероятность реализации угроз со стороны внутренних и внешних нарушителей. Итоговые выводы об актуальности угроз, сделанные с учетом реализованного комплекса мероприятий организационного и технического характера, снижающего вероятность реализации угроз со стороны внутренних и внешних нарушителей, и учитываемые при определении уточненных возможностей нарушителей и направления атак, а также необходимого уровня криптографической защиты информации, представлены в таблице «Уточненные актуальные угрозы безопасности» раздела «Оценка угроз в соответствии с методическими документами ФСБ России» Модели угроз.

5. Оценка угроз в соответствии с методическими документами ФСБ России

5.1. В соответствии с нормативными документами ФСБ России к объектам защиты, кроме защищаемой информации, относятся:

– средства криптографической защиты информации (далее – СКЗИ);

– среда функционирования СКЗИ (далее – СФ);

– информация, относящаяся к криптографической защите защищаемой информации, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

– документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИС и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФК;

– носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты защищаемой информации, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые в ИС каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите защищаемой информации.

5.2. В соответствии с нормативными документами ФСБ России все физические лица, имеющие доступ к техническим и программным средствам ИС, разделяются на следующие категории:

– лица, имеющие право постоянного доступа в контролируемую зону ИС (сотрудники, имеющие доступ к ИС, зарегистрированные пользователи ИС других организаций, обслуживающий персонал);

– лица, имеющие право разового доступа в контролируемую зону ИС (посетители и обслуживающий персонал, лица, осуществляющие ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ);

– привилегированные пользователи ИС;

– внешние источники атак.

5.3. Все потенциальные нарушители подразделяются на:

– внешних нарушителей, не имеющих доступа к ИС и осуществляющих атаки из-за пределов контролируемой зоны ИС;

– внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИС, включая пользователей ИС, и реализующих угрозы непосредственно в ИС.

5.4. Предполагается, что внешние источники атак, имеющие или не имеющие права доступа в контролируемую зону ИС, могут рассматриваться в качестве потенциальных источников атак.

5.5. Привилегированные пользователи – члены группы администраторов, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств СКЗИ и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями. К их числу относятся лица ответственные за обеспечение безопасности персональных данных в ИС и ответственный пользователь криптосредств.

5.6. Предполагается, что с использованием криптосредств безопасность информации необходимо обеспечивать только при передаче информации по каналам связи общего пользования, поэтому наличие потенциальных нарушителей возможно только среди категорий физических лиц, имеющих подключение к ИС. Предположение об отнесении категории нарушителей к потенциальным источникам атак представлены в таблице 8.

Таблица 8 – Предположение об отнесении категории нарушителей к потенциальным источникам атак

Категории нарушителей	**Вид нарушителя согласно Методике оценки УБИ от 05.02.2021**	**Предположение об отнесении категории нарушителей к потенциальным источникам атак**	**Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак**
Лица, имеющие право постоянного доступа в контролируемую зону объекта информатизации	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Да	Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Сведения о физических мерах защиты объектов, в которых размещена ИС, доступны ограниченному кругу сотрудников. Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты информации в металлическом сейфе (шкафу).

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
			Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками. Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода. Не установлены правила и процедуры доступа к машинным носителям информации. Не обеспечен учет машинных носителей информации, используемых в ИС для хранения и обработки информации. Не утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях. Не утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ. Доступ посторонних лиц в помещения с компонентами ИС допускается не только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом не предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемой информации и другим объектам защиты.

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
Лица, имеющие право постоянного доступа в контролируемую зону объекта информатизации	Авторизованные пользователи систем и сетей	Да	Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Сведения о физических мерах защиты объектов, в которых размещена ИС, доступны ограниченному кругу сотрудников. Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты информации в металлическом сейфе (шкафу). Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками. Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода. Не установлены правила и процедуры доступа к машинным носителям информации. Не обеспечен учет машинных носителей информации, используемых в ИС для хранения и обработки информации. Не установлены правила и процедуры управления учетными записями пользователей. Не установлены правила парольной защиты.

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
			Не установлены правила разграничения доступа. Не утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях. Не утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ. Доступ посторонних лиц в помещения с компонентами ИС допускается не только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом не предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемой информации и другим объектам защиты.
Лица, имеющие право разового доступа в контролируемую зону объекта информатизации	Разработчики программных, программно-аппаратных средств	Нет	Цели не предполагают потенциальное наличие нарушителя
Лица, имеющие право разового доступа в контролируемую	Поставщики вычислительных услуг, услуг связи	Да	Сведения о физических мерах защиты объектов, в которых размещена ИС, доступны ограниченному кругу сотрудников. Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
зону объекта информатизации			информации в металлическом сейфе (шкафу). Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками. Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода. Не утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях. Не утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ. Доступ посторонних лиц в помещения с компонентами ИС допускается не только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом не предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемой информации и другим объектам защиты. Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, находятся в этих помещениях не только в присутствии сотрудника ответственного за эксплуатацию СКЗИ.

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
Лица, имеющие право разового доступа в контролируемую зону объекта информатизации	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Да	Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ, выполняется не доверенными лицами, без выполнения мер по и обеспечению безопасности ПДн. Сведения о физических мерах защиты объектов, в которых размещена ИС, доступны ограниченному кругу сотрудников. Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты информации в металлическом сейфе (шкафу). Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками. Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода. Не утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях. Не утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ. Доступ посторонних лиц в помещения с компонентами ИС допускается не только в присутствии лиц, име-

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
			ющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом не предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемой информации и другим объектам защиты. Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, находятся в этих помещениях не только в присутствии сотрудника ответственного за эксплуатацию СКЗИ.
Привилегированные пользователи объекта информатизации	Системные администраторы и администраторы безопасности	Да	Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Ответственный за эксплуатацию средств криптографической защиты информации назначается не из числа особо доверенных лиц. Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты информации в металлическом сейфе (шкафу). Не установлены правила и процедуры доступа к машинным носителям информации. Не обеспечен учет машинных носителей информации, используемых в ИС для хранения и обработки информации.

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
			Не установлен перечень лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты информации. Не утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях. Не утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ. Доступ посторонних лиц в помещения с компонентами ИС допускается не только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом не предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемой информации и другим объектам защиты. Не проводятся работы по подбору сотрудников, привилегированные пользователи ИС назначаются не из числа доверенных лиц.
Внешние источники атак	Специальные службы иностранных государств	Нет	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.
Внешние источники атак	Террористические,	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений,

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
	экстремистские группировки		которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности.
Внешние источники атак	Преступные группы (криминальные структуры)	Да	
Внешние источники атак	Отдельные физические лица (хакеры)	Да	
Внешние источники атак	Конкурирующие организации	Нет	Конкурирующие организаций отсутствуют.
Внешние источники атак	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Да	Используются услуги непроверенных поставщиков. Не производится контроль целостности упаковки, пломб программных, программно-аппаратных средств, обеспечивающих систем.
Внешние источники атак	Бывшие (уволенные) работники	Да	

Категории нарушителей	Вид нарушителя согласно Методике оценки УБИ от 05.02.2021	Предположение об отнесении категории нарушителей к потенциальным источникам атак	Обоснование предположения об отнесении категории нарушителей к потенциальным источникам атак
	(пользо-ватели)		

5.7. На основании исходных данных о ИС, объектах защиты и источниках атак определены обобщенные возможности источников атак, которые описаны в таблице 9.

Таблица 9 – Обобщенные возможности источников атак

Обобщенная возможность источников атак	Предположение о возможности источников атак
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
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
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
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

5.8. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности информации определяется возможностями источников атак.

5.9. В рамках проводимых работ по созданию, разработке и внедрению системы защиты ИС, реализуется комплекс мероприятий организационного и технического характера, снижающий вероятность реализации угроз со стороны внутренних нарушителей.

5.10. С учетом реализованного комплекса мероприятий организационного и технического характера, снижающего вероятность реализации актуальных угроз, произведено уточнение перечня актуальных угроз, которое приведено в таблице 10.

Таблица 10 – Уточненные актуальные угрозы безопасности

Идентификатор угрозы	**Наименование угрозы**	**Принятые меры для нейтрализации угрозы**	**Актуальность угрозы с учетом принятых мер**
УБИ.004	Угроза аппаратного сброса пароля BIOS	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы). Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы). Помещения, в которых размещена ИС, оснащены механическими замками.	Да
УБИ.006	Угроза внедрения кода или данных	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Не используются сертифицированные средства защиты информации от НСД. Не реализовано управление идентификаторами пользователей и устройств в ИС. Не осуществляется контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей. Не осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.	Да
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Не реализовано управление идентификаторами пользователей и устройств в ИС.	Да
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не установлен перечень лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты информации. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Установлены пароли на BIOS/UEFI. Не используются сертифицированные средства анализа защищенности. Не реализовано управление идентификаторами пользователей и устройств в ИС. Не осуществляется контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей. Не осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.	Да
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства межсетевого экранирования. Не реализовано управление идентификаторами пользователей и устройств в ИС. Не осуществляется контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей. Не осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.	Да
УБИ.018	Угроза загрузки нештатной операционной системы	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Установлены пароли на BIOS/UEFI. Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы).	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Не используются сертифицированные средства защиты информации от НСД. Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы). Помещения, в которых размещена ИС, оснащены механическими замками. Не реализовано управление идентификаторами пользователей и устройств в ИС. Не осуществляется контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей. Не осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.	
УБИ.019	Угроза заражения DNS-кеша	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.022	Угроза избыточного выделения оперативной памяти	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да
УБИ.025	Угроза изменения системных и глобальных переменных	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила и процедуры доступа к машинным носителям информации.	Да
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Не реализовано управление идентификаторами пользователей и устройств в ИС. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Используется не доверенный источник обновлений BIOS.	Да
УБИ.033	Угроза использования слабостей кодирования входных данных	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Не используются сертифицированные средства анализа защищенности.	Да
УБИ.036	Угроза исследования механизмов работы программы	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не используются сертифицированные средства защиты информации от НСД. Помещения, в которых размещена ИС, оснащены механическими замками.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не используются сертифицированные средства защиты информации от НСД. Помещения, в которых размещена ИС, оснащены механическими замками. Не установлены правила разграничения доступа.	Да
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Не используются сертифицированные средства анализа защищенности.	Да
УБИ.041	Угроза межсайтового скриптинга	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.042	Угроза межсайтовой подделки запроса	Не используются сертифицированные средства защиты информации от НСД.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Не установлены правила и процедуры управления средствами аутентификации.	
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Не установлены правила разграничения доступа.	Да
УБИ.049	Угроза нарушения целостности данных кеша	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Не реализована настройка режимов энергосбережения.	Да
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Установлены пароли на BIOS/UEFI. Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы). Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы).	Нет
УБИ.061	Угроза некорректного задания структуры данных транзакции	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не используются сертифицированные средства защиты информации от НСД. Помещения, в которых размещена ИС, оснащены механическими замками. Не установлены правила разграничения доступа.	Да
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы). Не используются сертифицированные средства защиты информации от НСД. Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы). Помещения, в которых размещена ИС, оснащены механическими замками.	
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.069	Угроза неправомерных действий в каналах связи	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила и процедуры доступа к машинным носителям информации. Не обеспечивается уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.	
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Установлены пароли на BIOS/UEFI. Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Помещения, в которых размещена ИС, оснащены механическими замками. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них. Не установлены правила разграничения доступа.	Да
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
	и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети		
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила и процедуры доступа к машинным носителям информации. Не установлены правила разграничения доступа.	Да
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Не установлены правила разграничения доступа.	Да
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила и процедуры управления средствами аутентификации. Не установлены правила разграничения доступа.	Да
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Установлены пароли на BIOS/UEFI.	Нет

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы). Не используются сертифицированные средства защиты информации от НСД. Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы). Помещения, в которых размещена ИС, оснащены механическими замками.	Да
УБИ.089	Угроза несанкционированного редактирования реестра	Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Не установлены правила и процедуры управления учетными записями пользователей. Не установлены правила разграничения доступа.	Да
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы). Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Стойки и шкафы серверного и коммутационного оборудования закрыты и защищены от вскрытия (опечатаны/опломбированы). Помещения, в которых размещена ИС, оснащены механическими замками. Не установлены правила и процедуры резервного копирования защищаемой информации.	
УБИ.093	Угроза несанкционированного управления буфером	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да
УБИ.095	Угроза несанкционированного управления указателями	Не используются сертифицированные средства защиты информации от НСД.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.099	Угроза обнаружения хостов	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Не используются сертифицированные средства анализа защищенности. Не установлены правила и процедуры управления средствами аутентификации.	Да
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.103	Угроза определения типов объектов защиты	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.104	Угроза определения топологии вычислительной сети	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.109	Угроза перебора всех настроек и параметров приложения	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности. Не установлены правила парольной защиты.	Да
УБИ.111	Угроза передачи данных по скрытым каналам	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
	средств вычислительной техники	В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Помещения, в которых размещена ИС, оснащены механическими замками. Не установлены правила разграничения доступа.	
УБИ.114	Угроза переполнения целочисленных переменных	Работа пользователей ИС не регламентирована. Не установлены правила разграничения доступа.	Да
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.117	Угроза перехвата привилегированного потока	Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.118	Угроза перехвата привилегированного процесса	Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.121	Угроза повреждения системного реестра	Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да
УБИ.122	Угроза повышения привилегий	Не используются сертифицированные средства защиты информации от НСД. Не используются сертифицированные средства анализа защищенности.	Да
УБИ.123	Угроза подбора пароля BIOS	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не используются сертифицированные средства анализа защищенности. Помещения, в которых размещена ИС, оснащены механическими замками. Не установлены правила разграничения доступа.	Да
УБИ.124	Угроза подделки записей журнала регистрации событий	Не установлены правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них. Не установлены правила разграничения доступа.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.127	Угроза подмены действия пользователя путём обмана	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.	Да
УБИ.128	Угроза подмены доверенного пользователя	Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Работа пользователей ИС не регламентирована. Установлены пароли на BIOS/UEFI.	Да
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.131	Угроза подмены субъекта сетевого доступа	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да
УБИ.132	Угроза получения предварительной информации об объекте защиты	Не используются сертифицированные средства анализа защищенности.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Не используются сертифицированные средства межсетевого экранирования. Не используются сертифицированные средства обнаружения вторжений. Не установлены правила разграничения доступа.	
УБИ.139	Угроза преодоления физической защиты	Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.	Да
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.144	Угроза программного сброса пароля BIOS	Не установлены правила разграничения доступа.	Да
УБИ.145	Угроза пропуска проверки целостности	Не используются сертифицированные средства анализа защищенности.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
	программного обеспечения	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Не используются сертифицированные средства анализа защищенности.	Да
УБИ.150	Угроза сбоя процесса обновления BIOS	Не установлены правила разграничения доступа.	Да
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Не используются сертифицированные средства межсетевого экранирования. Не установлены правила разграничения доступа.	Да
УБИ.152	Угроза удаления аутентификационной информации	Не реализовано управление идентификаторами пользователей и устройств в ИС. Не установлены правила разграничения доступа.	Да
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Не используются сертифицированные средства межсетевого экранирования. Не установлены правила и процедуры резервного копирования защищаемой информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ, выполняется не доверенными лицами, без выполнения мер по и обеспечению безопасности ПДн. Не установлены правила разграничения доступа.	Да
УБИ.155	Угроза утраты вычислительных ресурсов	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.156	Угроза утраты носителей информации	Не установлены правила и процедуры доступа к машинным носителям информации. Не обеспечен учет машинных носителей информации, используемых в ИС для хранения и обработки информации.	Да
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Помещения, в которых размещена ИС, оснащены механическими замками.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.158	Угроза форматирования носителей информации	Работа пользователей ИС не регламентирована. Не установлены правила и процедуры доступа к машинным носителям информации. Не установлены правила и процедуры резервного копирования защищаемой информации. Не установлены правила разграничения доступа.	Да
УБИ.159	Угроза «форсированного веб-браузинга»	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Помещения, в которых размещена ИС, оснащены механическими замками.	Да
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Работа пользователей ИС не регламентирована.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства криптографической защиты информации. Не используются сертифицированные средства межсетевого экранирования.	Да
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Работа пользователей ИС не регламентирована.	Да
УБИ.166	Угроза внедрения системной избыточности	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Не установлены правила разграничения доступа.	Да
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Не используются сертифицированные средства анализа защищенности. Не реализовано управление идентификаторами пользователей и устройств в ИС. Не осуществляется контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей. Не осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.	Да
УБИ.169	Угроза наличия механизмов разработчика	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да
УБИ.170	Угроза неправомерного шифрования информации	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да
УБИ.171	Угроза скрытного включения вычислительного	Не используются сертифицированные средства анализа защищенности.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
	устройства в состав бот-сети	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	
УБИ.172	Угроза распространения «почтовых червей»	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да
УБИ.173	Угроза «спама» веб-сервера	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.174	Угроза «фарминга»	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.175	Угроза «фишинга»	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Работа пользователей ИС не регламентирована.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства анализа защищенности. Не установлены правила разграничения доступа.	Да
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Работа пользователей ИС не регламентирована. Не установлены правила и процедуры доступа к машинным носителям информации. Не установлены правила разграничения доступа.	Да
УБИ.182	Угроза физического устаревания аппаратных компонентов	Проводится периодическое техническое обслуживание основных и вспомогательных технических средств и систем ИС согласно эксплуатационной документации.	Нет
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	Да
УБИ.188	Угроза подмены программного обеспечения	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Не установлены правила разграничения доступа.	
УБИ.189	Угроза маскирования действий вредоносного кода	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. Не используются сертифицированные средства межсетевого экранирования. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Не используются сертифицированные средства анализа защищенности. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС. Работа пользователей ИС не регламентирована. В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
		Помещения, в которых размещена ИС, оснащены механическими замками. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Не используются сертифицированные средства анализа защищенности. Проводится периодическое техническое обслуживание основных и вспомогательных технических средств и систем ИС согласно эксплуатационной документации.	Да
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Не используются сертифицированные средства анализа защищенности. Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются. В ИС осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Не используются сертифицированные средства анализа защищенности.	Да
УБИ.212	Угроза перехвата управления информационной системой	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	Да
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Работа пользователей ИС не регламентирована. Не используются сертифицированные средства защиты информации от НСД. Не установлены правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них.	Да
УБИ.215	Угроза несанкционированного доступа к	Работа пользователей ИС не регламентирована.	Да

Идентификатор угрозы	Наименование угрозы	Принятые меры для нейтрализации угрозы	Актуальность угрозы с учетом принятых мер
	системе при помощи сторонних сервисов	Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Не используются сертифицированные средства защиты информации от НСД. Не установлены правила разграничения доступа.	
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Работа пользователей ИС не регламентирована. Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение. Проводится периодическое техническое обслуживание основных и вспомогательных технических средств и систем ИС согласно эксплуатационной документации. Не исключено использование скомпрометированных доверенных серверов обновлений программного обеспечения. Не установлены правила разграничения доступа.	Да

5.11. Исходя из обобщенных возможностей источников атак определены уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы). Результаты приведены в таблице 11.

Таблица 11 – Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС – Работа пользователей ИС не регламентирована – Ответственный за обеспечение безопасности ПДн, администраторы ИС назначаются из числа особо доверенных лиц – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ, выполняется не доверенными лицами, без выполнения мер по и обеспечению безопасности ПДн – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц – Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение – Не используются сертифицированные средства защиты информации от

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			НСД – Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются – Ответственный за эксплуатацию средств криптографической защиты информации назначается не из числа особо доверенных лиц
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, на которых реализованы СКЗИ и СФ	Да	– Ответственный за эксплуатацию средств криптографической защиты информации назначается не из числа особо доверенных лиц – Документация на СКЗИ не хранится у ответственного за эксплуатацию средств криптографической защиты информации в металлическом сейфе (шкафу) – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений	Да	– Работа пользователей ИС не регламентирована – Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	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		ответственности за их несоблюдение – Сведения о физических мерах защиты объектов, в которых размещена ИС, доступны ограниченному кругу сотрудников
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение	Да	– Работа пользователей ИС не регламентирована – Ответственный за обеспечение безопасности ПДн, администраторы ИС назначаются из числа особо доверенных лиц – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ, выполняется не доверенными лицами, без выполнения

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	и пресечение несанкционированных действий		мер по и обеспечению безопасности ПДн – Не проводится обучение пользователей ИС мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение – Не используются сертифицированные средства защиты информации от НСД – Пользователи ИС не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн – Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются – Программные, технические, программно-технические средства, в том числе и СЗИ, настроены не доверенными лицами и не соответствуют требованиям по и обеспечению безопасности ПДн
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИС, не имеют возможности находиться в помещениях, где расположена ИС, в отсутствие пользователей ИС – В помещениях, в которых происхо-

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			дит обработка ПДн, невозможно нахождение посторонних лиц – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие 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	Да	– В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц – Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы) – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО		стоимость и сложность подготовки реализации возможности
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	Нет	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	Нет	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

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	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		
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Нет	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
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	Возможность воздействовать на	Нет	Не осуществляется обработка сведений, составляющих государствен-

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	любые компоненты СКЗИ и СФ		ную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

6. Определение класса СКЗИ

6.1. В соответствии с Приказом ФСБ России № 378 от 10 июля 2014 г., методическими рекомендациями ФСБ России № 149/7/2/6-432 от 31 марта 2015 г., с учетом уточнения актуальности угроз, а также уточненными возможностями нарушителей и направлениями атак используемые для защиты информации СКЗИ должны обеспечить криптографическую защиту по уровню не ниже КС3.