ПРИЛОЖЕНИЕ

УТВЕРЖДЕНЫ
постановлением администрации района
от 02.02.2023 № 105

УГРОЗЫ
безопасности персональные данных, актуальных при обработке персональных данных в информационных системах персональных данных в администрации Первомайского района Тамбовской области и подведомственных ей организациях

1. Обозначения и сокращения

АП	–	Абонентский пункт
АРМ	–	Автоматизированное рабочее место
АС	–	Автоматизированная система
ЗИ	–	Защита информации
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
КЗ	–	Контролируемая зона
ЛВС	–	Локальная вычислительная сеть
МСПД	–	Межведомственная сеть передачи данных
НСД	–	Несанкционированный доступ
ОИ	–	Объект информатизации
ОС	–	Операционная система
ПДн	–	Персональные данные
ПЗУ	–	Постоянное запоминающее устройство
ПО	–	Программное обеспечение
ППЗУ	–	Программируемое ПЗУ
ПСВ	–	Протоколы сетевого взаимодействия
ПЭВМ	–	Персональная электронно-вычислительная машина
ПЭМИН	–	Побочные электромагнитные излучения и наводки
САВЗ	–	Средство антивирусной защиты
СВТ	–	Средства вычислительной техники
СЗИ	–	Средства защиты информации
СЗИ от НС	–	Средство защиты информации от несанкционированного доступа
ТК	–	Технический канал
ТКУИ	–	Технический канал утечки информации
ТС	–	Технические средства
УБИ	–	Угроза безопасности информации
УБПДн	–	Угроза безопасности персональных данных
УИТК	–	Утечка информации по техническим каналам
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю
BIOS	–	Базовая система ввода-вывода
UEFI	–	Расширяемый интерфейс встроенного ПО

2. Термины и определения

Автоматизированная обработка персональных данных– обработка персональных данных с помощью средств вычислительной техники.

Безопасность информации (данных) – состояние защищённости информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование доступа к информации – прекращение или затруднение доступа законных пользователей к 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.

Вредоносная программа (программное обеспечение) – программа(программное обеспечение), предназначенная для осуществления несанкционированного доступа и или деструктивного воздействия на информацию или ресурсы информационной системы нарушение их целостности и/или доступности.

Доступ к информации – возможность получения информации и её использования.

Доступность информации (ресурсов информационной системы) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами актами или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и или воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения сообщения, данные независимо от формы их представления.

Источник угрозы безопасности информации – субъект, физическое лицо, материальный объект или физическое явление, являющийся непосредственной причиной возникновения угрозы безопасности информации.

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

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

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

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Машинный носитель информации – материальный носитель, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами.

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

Модель угроз безопасности – это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Модификация информации – целенаправленное изменение формы представления и содержания информации.

Нарушитель безопасности информации – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Недекларированные возможности (программного обеспечения) – функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и (или) целостности обрабатываемой информации.

Несанкционированный доступ к информации – доступ к информации ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Предоставление информации – действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц.

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства криптографической защиты информации - средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования - 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.

Средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

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

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

Уязвимость – слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз.

Уязвимость программного обеспечения – ошибка в программном обеспечении, способная напрямую быть использована хакером для получения доступа к системе или сети.

Целостность информации – состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и (или) непреднамеренного воздействия на нее.

3. Нормативные и библиографические ссылки

Настоящий документ составлен в соответствии и на основании следующих документов:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»(утверждены приказом ФСТЭК России от 18 февраля 2013 г.).
- Методический документ «Методика оценки угроз безопасности информации» (утвержденный ФСТЭК России 5 февраля 2021 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (утверждён приказом ФСБ России 10 июля 2014 г. №378).
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены Приказом начальника 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432)
- Банк данных угроз безопасности информации www.bdu.fstec.ru

4. Общие положения

Настоящий документ (далее – Модель угроз) описывает возможные угрозы безопасности, которым подвержен ОИ «АРМ-АИСТ».

Модель угроз содержит данные по УБПДн, реализация которых может привести к нарушению безопасности ПДн, обрабатываемых на ОИ.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Разработка Модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности ПДн, обрабатываемых в ИСПДн, и проектирования СЗПДн.

Модель угроз необходима для:

- анализа защищённости ИСПДн от УБПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

- разработки СЗИ ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием мер по обеспечению безопасности ПДн, предусмотренных для соответствующего уровня защищённости ПДн;
- проведения мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи ПДн лицам, не имеющим права доступа к ПДн;
- недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроля (мониторинга) за обеспечением уровня защищённости ПДн, обрабатываемых в ИСПДн.

В Модели угроз представлено описание ИСПДн и её структурно-функциональных характеристик, описание УБПДн, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации УБПДн и последствий от нарушения свойств безопасности информации, а также произведён анализ УБПДн.

Анализ УБПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

В процессе функционирования ИСПДн, предполагается конкретизировать и пересматривать данную Модель угроз.

УБПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых уязвимостей, источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Модель угроз может быть пересмотрена:

- на основе периодически проводимых анализа и оценки УБПДн с учетом особенностей и (или) изменений ИСПДн;
- по результатам мероприятий по контролю за выполнением требований по защите информации в ИСПДн.

Оператор системы «АРМ-АИСТ» - администрация Первомайского района Тамбовской области.

Модель угроз безопасности информации разработана совместно с администратором безопасности и ООО «Тигрис».

5. Описание информационных систем и особенности их функционирования

Настоящая модель угроз разработана для информационной системы «АРМ-АИСТ» функционирующая в администрации Первомайского района Тамбовской области.

В ИС «АРМ-АИСТ» обрабатывают следующие типы персональных данных представлены в таблице.

Таблица 1 – Типы ПДн, входящие в ИС

Наименование ИС	Типы ПДн, обрабатываемые в ИС
«АРМ-АИСТ»	− Фамилия, имя, отчество, дата и место рождения − Паспортные данные (серия, номер, дата выдачи, наименование органа, выдавшего документ) − Реквизиты свидетельства о рождении (серия, номер, дата выдачи и орган, выдавший документ)

	− Адрес места регистрации, дата регистрации по месту жительства или по месту пребывания, адрес фактического места жительства − Контактный телефон − Гражданство; национальность − Данные о состоянии здоровья (диагнозы, заключение областной психолого-медико-педагогической комиссии об умственном развитии, наличие инвалидности) − Данные о родителях и ближайших родственниках (фамилия, имя, отчество, дата рождения, адрес) − Семейное положение − Этническое происхождение − Особенности характера − Реквизиты документов об установлении усыновления, опеки, приемной семьи − Сведения о наличии движимого и недвижимого имущества (вид и наименование имущества, основания приобретения, местонахождение (адрес, площадь, сведения о государственной регистрации права на имущество) − Денежные средства, находящиеся на счетах в кредитных организациях (наименование и адрес кредитной организации, вид и валюта счета, дата открытия счета, номер счета) − Наличие ценных бумаг (вид ценной бумаги, наименование и организационно-правовая форма организации, местонахождение организации (адрес), лицо, выпустившее ценную бумагу) − Сведения о доходах несовершеннолетнего (вид дохода алименты, пенсии, пособия, единовременные страховые выплаты и иные виды доходов, основания для получения).

ИС обрабатывает специальные категории ПДн, в том числе персональные данные сотрудников оператора, менее чем 100000 субъектов ПДн.

Назначение «АРМ-АИСТ» – обеспечение конфиденциальности информации о детях, оставшихся без попечения.

Целями обработки ПДн в ИСПДн являются:

- учет сведений о детях, оставшихся без попечения родителей, проживающих на территории области и подлежащих устройству на воспитание в семью;
- учет граждан, выразивших желание принять детей на воспитание в семью (кандидаты в усыновители, опекуны (попечители));
- обеспечение оперативной актуализации сведений о детях, оставшихся без попечения родителей;
- создание условий для эффективного взаимодействия между органами исполнительной власти субъектов Российской Федерации, исполняющих функции региональных операторов государственного банка данных о детях, оставшихся без попечения родителей, Минобрнауки России и органами опеки и попечительства.

В ИСПДн «АРМ-АИСТ» в отношении ПДн осуществляются следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление), удаление.

Режим обработки ПДн – многопользовательский с равными правами доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

Обработка ПДн осуществляется в смешанном виде (с использованием средств автоматизации и без использования средств автоматизации).

Технические средства ИСПДн располагаются по адресу: 393700, Тамбовская область, Первомайский район, р.п. Первомайский, пл. Ленина, д.11, первый этаж, каб.110.

Объектами защиты в ИСПДн «АРМ-АИСТ» являются: машинные носители информации, программное и аппаратное обеспечение, информационные ресурсы.

Комплекс технических средств АС включает средства обработки данных, такие как:

- ПЭВМ;
- средства обмена данными в ЛВС (кабельная система, и т.д.);
- системы хранения данных, системы архивирования/восстановления.

Получение ПДн происходит непосредственно от субъекта ПДн и подведомственных учреждений.

В процессе обработки ПДн хранятся на накопителе на жёстких дисках АП и съёмных машинных носителях ПДн (флэш-накопители).

В ИСПДн применяются съемные машинные носители: флэш-накопители.

ИС «АРМ-АИСТ» взаимодействует с информационно-телекоммуникационным сетями международного информационного обмена.

В ИС отсутствуют беспроводные каналы передачи информации.

В ИС не применяются технические средства, обрабатывающие акустическую информацию (микрофоны, наушники, акустические колонки).

Структурная схема подключения ОИ и его внешних связей представлена на рисунке 1.

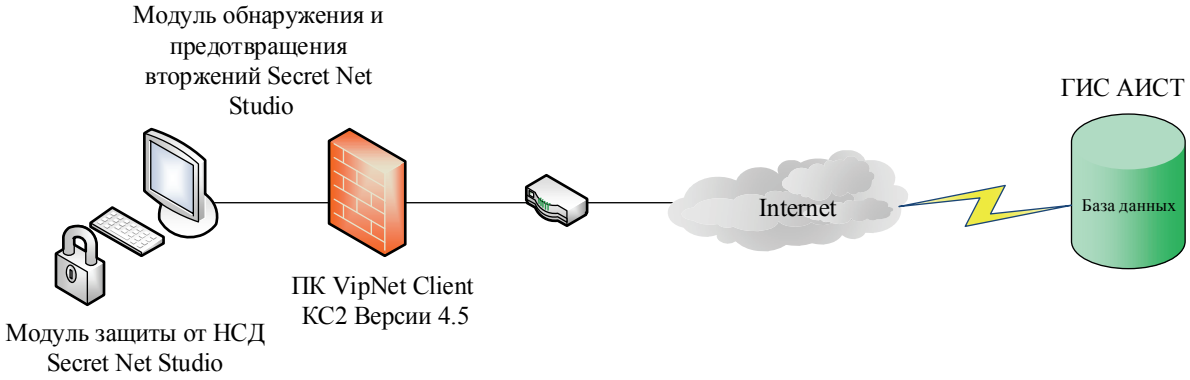

Рисунок 1 – Схема подключения «АРМ-АИСТ» ИС

КЗ ИС является она, граница которой проходит по внешнему периметру ограждающих конструкций помещений. Схема контролируемой зоны представлена на рисунке № 2.

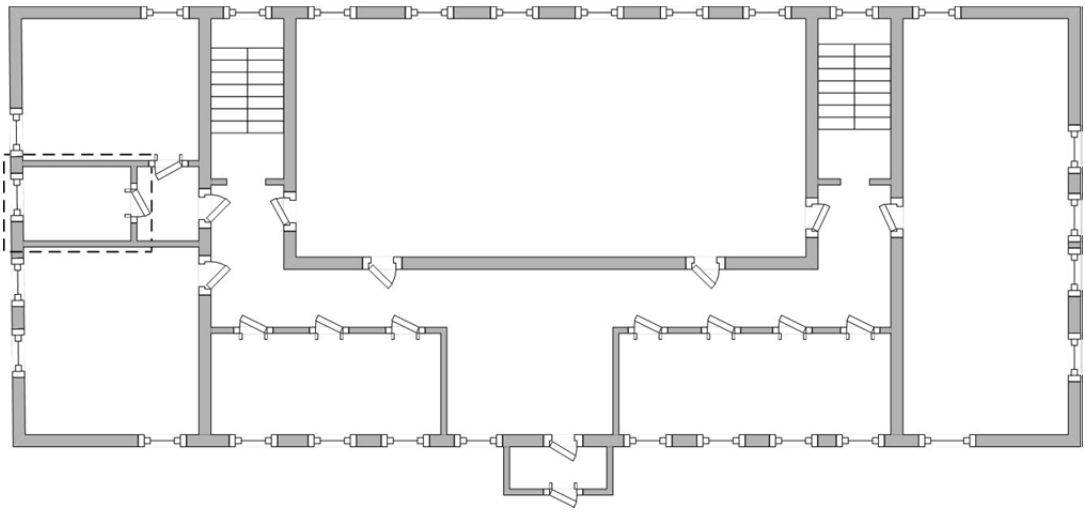

Рисунок 2 – Схема КЗ ИС

6. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Для определения негативных последствий от реализации угроз безопасности информации, необходимо использовать следующие исходные данные:

1) общий перечень угроз безопасности информации, содержащиеся в банке данных угроз безопасности ФСТЭК России (bdu.fstek.ru);
2) нормативные правовые акты РФ;
3) документация на сети и системы;
4) технологические, производственные карты и иные документы, содержащие описание основных процессов обладателя информации, оператора;
5) результаты оценки рисков.

На основании анализа исходных данных на ОИ «АРМ-АИСТ», возможные реализации угроз приведены в таблице 2.

Таблица 2 – виды риска (ущерба) и типовые негативные последствия

№	Виды риска (ущерба)	Возможные типовые негативные последствия
1	Ущерб физическому лицу	Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан

7. Возможные объекты воздействия угроз безопасности информации

В таблице 3 приведен перечень объектов воздействия в соответствии с Банком данных угроз безопасности информации. В столбце «Применимость» ставится знак «+», если данный объект воздействия существует или может появится в рассматриваемом ОИ «АРМ-АИСТ». При определении возможных актуальных угроз безопасности рассматриваются только те объекты воздействия, у которых в столбце «Применимость» стоит знак «+».

Таблица 3 – Объекты воздействия угроз

№ п.п.	Объект воздействия	Применимость
1.	Аппаратное обеспечение	+
2.	Аппаратное устройство	+
3.	Виртуальная машина	-
4.	Виртуальные устройства	-
5.	Гипервизор	-
6.	Грид-система	-
7.	Информационная система	+
8.	Каналы связи (передачи) данных	+
9.	Машинный носитель информации	+
10.	Микропрограммное обеспечение BIOS/UEFI	+
11.	Мобильное устройство	-

12.	Носитель информации	+
13.	Облачная инфраструктура	-
14.	Объекты файловой системы	+
15.	Прикладное программное обеспечение	+
16.	Рабочая станция	+
17.	Реестр	+
18.	Сервер	-
19.	Сетевое программное обеспечение	-
20.	Сетевой трафик	+
21.	Сетевой узел	+
22.	Системное программное обеспечение	-
23.	Средство вычислительной техники	+
24.	Средство защиты информации	-
25.	Суперкомпьютер	-
26.	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	-
27.	Учётные данные пользователя	+
28.	Хранилище больших данных, метаданные	+

В таблице 4 определены объекты воздействия и возможные виды воздействия на объект информатизации «АРМ-АИСТ», согласно ранее выбранным негативным последствиям.

Таблица 4 – Объекты воздействия

Негативные последствия	**Объекты воздействия**	**Виды воздействия**
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы

8. Источники угроз безопасности информации

В зависимости от имеющихся прав доступа нарушители имеют санкционированный физический и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не имеют такого доступа.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы (ее контролируемой зоны);

внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Угрозы безопасности информации в «АРМ-АИСТ» могут быть реализованы следующими видами и типами нарушителей, представленными в таблице 5**Ошибка! Источник ссылки не найден.**.

Таблица 5 – Виды нарушителей информационной безопасности

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1.	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
2.	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
3.	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия
4.	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия

В таблице 6 представлены возможные негативные последствия и виды рисков (ущерба) от их реализации (возникновения).

Таблица 6 – Соответствие видов нарушителей, возможных целей реализаций ими угроз безопасности информации и возможные негативные последствия

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Отдельные физические лица (хакеры)	+ (желание самореализоваться)	-	-	У1 (Нарушение конфиденциальности (утечка) персональных данных) (Финансовый, иной материальный ущерб физическому лицу)
Авторизованные пользователи систем и сетей	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	-	У1 (Нарушение конфиденциальности (утечка) персональных данных)

				(Разглашение персональных данных граждан)
Системные администраторы и администраторы безопасности	+ (любопытство или желание самореализации)	-	-	У1 (Нарушение конфиденциальности (утечка) персональных данных)
Бывшие (уволенные) работники (пользователи)	+ (месть за ранее совершенные действия)	-	-	У1 (Разглашение персональных данных граждан)-

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. Потенциал нарушителей и их возможности приведены в таблице 7**Ошибка! Источник ссылки не найден.**.

Таблица 7 – Уровни возможностей нарушителей

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз	Преступные группы (два лица и более, действующие по единому плану)

		(инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	Конкурирующие организации Поставщики вычислительных услуг, услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы безопасности
Н3	Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и	Террористические, экстремистские группировки Разработчики программных, программно-аппаратных средств

		инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	
Н4	Нарушитель, обладающий высокими	Обладает всеми возможностями нарушителей со средними возможностями.	Специальные службы иностранных государств

	возможностями	Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных	

		защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей	

Исходя из перечня доверенных лиц, технологии обработки информации, архитектуры, технических особенностей «АРМ-АИСТ», организационно-штатной структуры оператора и характера взаимоотношений с внешними организациями проведена оценка актуальности потенциальных нарушителей. Результаты оценки приведены в таблице 8.

Таблица 8 – Оценка актуальности категорий нарушителей

№ вида	Вид нарушителя	Идентификатор нарушителя	Актуальность использования возможностей нарушителя для построения и реализации атак	Обоснование отсутствия
1	Специальные службы иностранных государств (блоков государств)	Р1	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителем
2	Террористические, экстремистские группировки	Р2	Не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности нарушителем
3	Преступные группы (криминальные структуры)	Р3	Не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности нарушителем
4	Внешние субъекты	Р4	Актуально	-
5	Конкурирующие организации	Р5	Не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности нарушителем. Отсутствие конкурирующих организаций

№ вида	Вид нарушителя	Идентификатор нарушителя	Актуальность использования возможностей нарушителя для построения и реализации атак	Обоснование отсутствия
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Р6	Не актуально	Разработчики, производители, поставщики программных, технических и программно-технических средств отнесены к доверенным лицам. Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности нарушителем. Выбор доверенных разработчиков, производителей и поставщиков. Выполнение работ организациями с наличием лицензий в соответствии с действующим законодательством Российской Федерации
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Р7	Не актуально	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ отнесены к доверенным лицам
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора	Р8	Не актуально	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора отнесены к доверенным лицам
9	Пользователи информационной системы	Р9	Актуально	-

№ вида	Вид нарушителя	Идентификатор нарушителя	Актуальность использования возможностей нарушителя для построения и реализации атак	Обоснование отсутствия
10	Администраторы информационной системы и администраторы безопасности	Р10	Актуально	-
11	Бывшие работники (пользователи)	Р11	Актуально	-

В соответствии с проведенной оценкой актуальности нарушителей безопасности информации в «АРМ-АИСТ»:

потенциальный сговор нарушителей 1,2,3 видов (Н1, Н2) с актуальными видами нарушителей (Р4, Р9, Р10, Р11) в «АРМ-АИСТ» далее не рассматривается;

угрозы безопасности информации в «АРМ-АИСТ» могут быть реализованы:

внешними нарушителями с базовым (низким) потенциалом (Р4, Р11);

внутренними нарушителями с базовым (низким) потенциалом (Р9, Р10).

9. Способы реализации (возникновения) угроз безопасности информации

Результаты оценки приведены в таблице 9

Таблица 9 – Способы реализации угроз безопасности

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
Т2	Получение первоначального доступа к компонентам систем и сетей Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств,

	получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий	содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций. Примеры: 1) передача флеш-носителя в комплекте материалов выездного мероприятия; 2) подмена USB-адаптера беспроводной клавиатуры схожим внешне, но реализующим функции сбора и передачи данных устройством
		Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
		Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
Т6	Повышение привилегий по доступу к компонентам систем и сетей Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом	Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий. Пример: эксплуатация уязвимости драйвера службы печати, позволяющей выполнить код с привилегиями системной учетной записи, через доступ к этому драйверу из приложения, запущенного от имени непривилегированного пользователя
		Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима. Пример: обход UserAccountControl в операционной системе Windows
		Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с

		повышенными привилегиями. Примеры: 1) использование профилей PowerShell для закрепления вредоносного ПО в системе и выполнения этого ПО с повышенными привилегиями; 2) конфигурация команды перехода в привилегированный режим sudo, при которой успешный результат выполнения этой команды на некоторое время кэшируется, что при определенных обстоятельствах может быть использовано вредоносным кодом для выполнения привилегированных операций в течение этого времени; 3) параметры исполнения файлов (ImageFileExecutionOptions, IFEO), позволяющие переключать исполнение файлов в режим отладки, выполняя вредоносные приложения под видом отладчиков и средств мониторинга, что позволяет им отключать системные приложения и средства защиты
		Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей. Пример: подмена на диске бинарных файлов или скриптов, предназначенных для исполнения в привилегированном контексте, приложением, исполняющимся в непривилегированном контексте
		Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения. Пример: использование популярной утилиты PsExec для ОС Windows как администраторами, так и нарушителями
Т7	Сокрытие действий и применяемых при этом средств от обнаружения Тактическая задача: нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их	Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
		Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и

		управляемого (контролируемого) объекта и (или) процесса
		Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе.
		Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.
		Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.
		Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах.
		Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы

10. Актуальны угрозы безопасности информации

В данной Модели угроз используется перечень и описание угроз безопасности в соответствии со следующими источниками:
Постановление Правительства № 1119;
Банк данных угроз;
Базовая модель угроз.
Общий перечень угроз безопасности информации представлен в таблице Таблица 10.

Таблица 10 – Общий перечень угроз безопасности информации

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном программном обеспечении	Постановление Правительства № 1119
ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	Постановление Правительства № 1119
ДОП.003	Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	Базовая модель угроз
ДОП.004	Природные угрозы	Базовая модель угроз
ДОП.005	Техногенные угрозы	Базовая модель угроз
ДОП.006	Угроза утечки акустической (речевой) информации	Базовая модель угроз
ДОП.007	Угроза утечки видовой информации	Базовая модель угроз
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Банк данных угроз
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Банк данных угроз
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	Банк данных угроз
УБИ.004	Угроза аппаратного сброса пароля BIOS	Банк данных угроз
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Банк данных угроз
УБИ.006	Угроза внедрения кода или данных	Банк данных угроз
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Банк данных угроз
УБИ.008	Угроза восстановления аутентификационной информации	Банк данных угроз
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Банк данных угроз
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Банк данных угроз
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Банк данных угроз
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Банк данных угроз
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Банк данных угроз
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Банк данных угроз
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Банк данных угроз
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Банк данных угроз
УБИ.018	Угроза загрузки нештатной операционной системы	Банк данных угроз
УБИ.019	Угроза заражения DNS-кеша	Банк данных угроз
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Банк данных угроз
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Банк данных угроз
УБИ.022	Угроза избыточного выделения оперативной памяти	Банк данных угроз
УБИ.023	Угроза изменения компонентов системы	Банк данных угроз
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Банк данных угроз
УБИ.025	Угроза изменения системных и глобальных переменных	Банк данных угроз
УБИ.026	Угроза искажения XML-схемы	Банк данных угроз
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Банк данных угроз
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Банк данных угроз
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Банк данных угроз
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Банк данных угроз
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Банк данных угроз
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Банк данных угроз
УБИ.033	Угроза использования слабостей кодирования входных данных	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Банк данных угроз
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Банк данных угроз
УБИ.036	Угроза исследования механизмов работы программы	Банк данных угроз
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Банк данных угроз
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Банк данных угроз
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Банк данных угроз
УБИ.040	Угроза конфликта юрисдикций различных стран	Банк данных угроз
УБИ.041	Угроза межсайтового скриптинга	Банк данных угроз
УБИ.042	Угроза межсайтовой подделки запроса	Банк данных угроз
УБИ.043	Угроза нарушения доступности облачного сервера	Банк данных угроз
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Банк данных угроз
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Банк данных угроз
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Банк данных угроз
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Банк данных угроз
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Банк данных угроз
УБИ.049	Угроза нарушения целостности данных кеша	Банк данных угроз
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Банк данных угроз
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Банк данных угроз
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Банк данных угроз
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Банк данных угроз
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Банк данных угроз
УБИ.055	Угроза незащищённого администрирования облачных услуг	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Банк данных угроз
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Банк данных угроз
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Банк данных угроз
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Банк данных угроз
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Банк данных угроз
УБИ.061	Угроза некорректного задания структуры данных транзакции	Банк данных угроз
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Банк данных угроз
УБИ.063	Угроза некорректного использования функционала программного обеспечения	Банк данных угроз
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Банк данных угроз
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Банк данных угроз
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Банк данных угроз
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Банк данных угроз
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Банк данных угроз
УБИ.069	Угроза неправомерных действий в каналах связи	Банк данных угроз
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Банк данных угроз
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Банк данных угроз
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Банк данных угроз
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Банк данных угроз
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Банк данных угроз
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Банк данных угроз
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Банк данных угроз
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Банк данных угроз
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Банк данных угроз
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Банк данных угроз
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Банк данных угроз
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Банк данных угроз
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Банк данных угроз
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Банк данных угроз
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Банк данных угроз
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Банк данных угроз
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Банк данных угроз
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Банк данных угроз
УБИ.089	Угроза несанкционированного редактирования реестра	Банк данных угроз
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Банк данных угроз
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Банк данных угроз
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Банк данных угроз
УБИ.093	Угроза несанкционированного управления буфером	Банк данных угроз
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Банк данных угроз
УБИ.095	Угроза несанкционированного управления указателями	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Банк данных угроз
УБИ.097	Угроза несогласованности правил доступа к большим данным	Банк данных угроз
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Банк данных угроз
УБИ.099	Угроза обнаружения хостов	Банк данных угроз
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Банк данных угроз
УБИ.101	Угроза общедоступности облачной инфраструктуры	Банк данных угроз
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Банк данных угроз
УБИ.103	Угроза определения типов объектов защиты	Банк данных угроз
УБИ.104	Угроза определения топологии вычислительной сети	Банк данных угроз
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Банк данных угроз
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Банк данных угроз
УБИ.107	Угроза отключения контрольных датчиков	Банк данных угроз
УБИ.108	Угроза ошибки обновления гипервизора	Банк данных угроз
УБИ.109	Угроза перебора всех настроек и параметров приложения	Банк данных угроз
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Банк данных угроз
УБИ.111	Угроза передачи данных по скрытым каналам	Банк данных угроз
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Банк данных угроз
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Банк данных угроз
УБИ.114	Угроза переполнения целочисленных переменных	Банк данных угроз
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Банк данных угроз
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Банк данных угроз
УБИ.117	Угроза перехвата привилегированного потока	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.118	Угроза перехвата привилегированного процесса	Банк данных угроз
УБИ.119	Угроза перехвата управления гипервизором	Банк данных угроз
УБИ.120	Угроза перехвата управления средой виртуализации	Банк данных угроз
УБИ.121	Угроза повреждения системного реестра	Банк данных угроз
УБИ.122	Угроза повышения привилегий	Банк данных угроз
УБИ.123	Угроза подбора пароля BIOS	Банк данных угроз
УБИ.124	Угроза подделки записей журнала регистрации событий	Банк данных угроз
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Банк данных угроз
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Банк данных угроз
УБИ.127	Угроза подмены действия пользователя путём обмана	Банк данных угроз
УБИ.128	Угроза подмены доверенного пользователя	Банк данных угроз
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Банк данных угроз
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Банк данных угроз
УБИ.131	Угроза подмены субъекта сетевого доступа	Банк данных угроз
УБИ.132	Угроза получения предварительной информации об объекте защиты	Банк данных угроз
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Банк данных угроз
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Банк данных угроз
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Банк данных угроз
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Банк данных угроз
УБИ.137	Угроза потери управления облачными ресурсами	Банк данных угроз
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Банк данных угроз
УБИ.139	Угроза преодоления физической защиты	Банк данных угроз
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Банк данных угроз
УБИ.141	Угроза привязки к поставщику облачных услуг	Банк данных угроз
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз
УБИ.144	Угроза программного сброса пароля BIOS	Банк данных угроз
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Банк данных угроз
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Банк данных угроз
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Банк данных угроз
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Банк данных угроз
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Банк данных угроз
УБИ.150	Угроза сбоя процесса обновления BIOS	Банк данных угроз
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Банк данных угроз
УБИ.152	Угроза удаления аутентификационной информации	Банк данных угроз
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Банк данных угроз
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Банк данных угроз
УБИ.155	Угроза утраты вычислительных ресурсов	Банк данных угроз
УБИ.156	Угроза утраты носителей информации	Банк данных угроз
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз
УБИ.158	Угроза форматирования носителей информации	Банк данных угроз
УБИ.159	Угроза «форсированного веб-браузинга»	Банк данных угроз
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Банк данных угроз
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Банк данных угроз
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Банк данных угроз
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Банк данных угроз
УБИ.166	Угроза внедрения системной избыточности	Банк данных угроз
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Банк данных угроз
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Банк данных угроз
УБИ.169	Угроза наличия механизмов разработчика	Банк данных угроз
УБИ.170	Угроза неправомерного шифрования информации	Банк данных угроз
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Банк данных угроз
УБИ.172	Угроза распространения «почтовых червей»	Банк данных угроз
УБИ.173	Угроза «спама» веб-сервера	Банк данных угроз
УБИ.174	Угроза «фарминга»	Банк данных угроз
УБИ.175	Угроза «фишинга»	Банк данных угроз
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Банк данных угроз
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Банк данных угроз
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Банк данных угроз
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Банк данных угроз
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Банк данных угроз
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Банк данных угроз
УБИ.182	Угроза физического устаревания аппаратных компонентов	Банк данных угроз
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Банк данных угроз
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Банк данных угроз
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Банк данных угроз
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Банк данных угроз
УБИ.188	Угроза подмены программного обеспечения	Банк данных угроз
УБИ.189	Угроза маскирования действий вредоносного кода	Банк данных угроз
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Банк данных угроз
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Банк данных угроз
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Банк данных угроз
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Банк данных угроз
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Банк данных угроз
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Банк данных угроз
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Банк данных угроз
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Банк данных угроз
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Банк данных угроз
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Банк данных угроз
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Банк данных угроз
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Банк данных угроз
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Банк данных угроз
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Банк данных угроз
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Банк данных угроз
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Банк данных угроз
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Банк данных угроз
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Банк данных угроз
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Банк данных угроз
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Банк данных угроз
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечениям администрирования информационных систем	Банк данных угроз
УБИ.212	Угроза перехвата управления информационной системой	Банк данных угроз
УБИ.213	Угроза обхода многофакторной аутентификации	Банк данных угроз
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Банк данных угроз
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Банк данных угроз
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Банк данных угроз
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Банк данных угроз
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Банк данных угроз
УБИ.219	Угроза хищения обучающих данных	Банк данных угроз
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Банк данных угроз
УБИ.222	Угроза подмены модели машинного обучения	Банк данных угроз

11. Систематизированный перечень угроз безопасности информации

Объекты воздействия приведены для каждой угрозы безопасности информации в Банке данных угроз.

В рамках систематизации угроз безопасности информации, общий перечень угроз безопасности информации в соответствии с возможными архитектурными уровнями разделяется на следующие группы:

Уровень обеспечения системного ПО (1);

Уровень обеспечения прикладного ПО (2);

Уровень обеспечения внутреннего сетевого взаимодействия (3);

Уровень обеспечения внешнего сетевого взаимодействия (4);

Уровень обеспечения АРМ (5).

Общий перечень угроз безопасности информации (УБИ) декомпозированный по архитектурным уровням представлен в таблице 11.

Таблица 11 – Угрозы информационной безопасности в соответствии с архитектурными уровнями

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	+	-	-	-	+
ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	-	+	-	-	+
ДОП.003	Угрозы утечки информации по каналу ПЭМИН	-	-	+	+	+
ДОП.004	Природные угрозы	-	-	+	+	+
ДОП.005	Техногенные угрозы	-	-	+	+	+
ДОП.006	Угроза утечки акустической (речевой) информации	-	-	+	+	+
ДОП.007	Угроза утечки видовой информации	-	-	-	-	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	-	-	-	-	-
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	-	-	-	+	-
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	+	+	-	+	+
УБИ.004	Угроза аппаратного сброса пароля BIOS	-	-	-	-	+
УБИ.005	Угроза внедрения вредоносного кода в BIOS	-	-	+	+	+
УБИ.006	Угроза внедрения кода или данных	+	+	+	+	+
УБИ.007	Угроза воздействия на программы с высокими привилегиями	+	+	+	+	+
УБИ.008	Угроза восстановления аутентификационной информации	+	+	+	+	+
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	-	-	+	+	+
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	+	-	-	-	-
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	-	-	+	+	+
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.017	Угроза доступа/перехвата/изменения HTTP cookies	-	+	+	+	+
УБИ.018	Угроза загрузки нештатной операционной системы	-	-	+	+	+
УБИ.019	Угроза заражения DNS-кеша	+	-	+	+	+
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	-	-	-	-	-
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	-	-	-	-	-
УБИ.022	Угроза избыточного выделения оперативной памяти	+	-	-	-	+
УБИ.023	Угроза изменения компонентов системы	+	+	+	+	+
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	-	-	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.025	Угроза изменения системных и глобальных переменных	+	+	+	+	+
УБИ.026	Угроза искажения XML-схемы	-	-	+	+	+
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	+	+	+	+	+
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	+	+	+	+	+
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	+	-	-	-	-
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	+	+	+	+	+
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	+	-	+	+	+
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	-	-	+	+	+
УБИ.036	Угроза исследования механизмов работы программы	+	+	+	+	+
УБИ.037	Угроза исследования приложения через отчёты об ошибках	+	+	+	+	+
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	+	+	+	+	+
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	-	-	+	+	+
УБИ.040	Угроза конфликта юрисдикций различных стран	-	-	-	-	-
УБИ.041	Угроза межсайтового скриптинга	-	-	+	+	+
УБИ.042	Угроза межсайтовой подделки запроса	-	+	+	+	+
УБИ.043	Угроза нарушения доступности облачного сервера	-	-	-	-	-
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	-	-	-	-	-
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	-	-	+	+	+
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	+	+	+	+	-

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	-	-	-	+	-
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	-	-	+	+	-
УБИ.049	Угроза нарушения целостности данных кеша	+	+	-	+	+
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	-	+	-	-	-
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	+	+	-	-	+
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	+	-	-	-	-
УБИ.053	Угроза невозможности управления правами пользователей BIOS	-	-	+	+	+
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	+	+	+	+	+
УБИ.055	Угроза незащищённого администрирования облачных услуг	-	-	+	+	+
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	+	-	-	-	-
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	+	+	+	-	-
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	-	-	-	-	-
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	-	-	-	-	-
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	+	+	+	-	-
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 обеспечения	+	+	+	+	+
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	-	+	+	+	+
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	-	-	-	-	-
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	-	-	-	-	-
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	+	-	-	-	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	+	+	+	+	+
УБИ.069	Угроза неправомерных действий в каналах связи	-	-	+	+	-
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	-	-	-	-	-
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.075	Угроза несанкционированного доступа к виртуальным каналам передачи	-	-	-	+	+
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	-	-	+	-	-
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	-	+	-	-	-
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	-	-	-	-	-
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	-	-	-	-	-
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	-	-	+	-	-
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	-	-	-	-	-
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	-	-	-	-	-
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	+	+	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	-	-	-	-	-
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.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	+	+	+	+	+
УБИ.093	Угроза несанкционированного управления буфером	+	+	+	+	+
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	+	+	+	+	+
УБИ.095	Угроза несанкционированного управления указателями	+	+	+	+	+
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	+	-	-	-	-
УБИ.097	Угроза несогласованности правил доступа к большим данным	-	-	-	-	-
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	-	-	+	+	+
УБИ.099	Угроза обнаружения хостов	-	-	+	+	+
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	+	-	+	+	+
УБИ.101	Угроза общедоступности облачной инфраструктуры	+	-	-	-	-
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	-	-	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	-	+	-	-	-
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	-	-	-	-	-
УБИ.107	Угроза отключения контрольных датчиков	+	-	-	-	-
УБИ.108	Угроза ошибки обновления гипервизора	-	-	-	-	-
УБИ.109	Угроза перебора всех настроек и параметров приложения	+	+	+	+	+
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	-	-	-	-	-
УБИ.111	Угроза передачи данных по скрытым каналам	-	-	+	+	+
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	+	+	+	-	-
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.119	Угроза перехвата управления гипервизором	+	-	+	-	-
УБИ.120	Угроза перехвата управления средой виртуализации	+	+	+	+	+
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.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	-	-	+	+	+
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	-	-	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
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.133	Угроза получения сведений о владельце беспроводного устройства	-	+	+	+	+
УБИ.134	Угроза потери доверия к поставщику облачных услуг	+	+	+	+	+
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	+	+	+	+	+
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	+	+	+	+	+
УБИ.137	Угроза потери управления облачными ресурсами	+	-	+	+	+
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	+	+	+	+	+
УБИ.139	Угроза преодоления физической защиты	-	-	-	-	+
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	+	+	+	+	-
УБИ.141	Угроза привязки к поставщику облачных услуг	+	+	+	+	+
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	-	-	+	+	+
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.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	+	-	+	+	+
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	-	-	-	+	+
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	+	+	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
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	-	+	+	+	+
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.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	-	-	-	-	-
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	+	+	-	-	+
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	+	-	-	-	+
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	-	-	-	-	-
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	+	+	+	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
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.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	+	+	+	+	+
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.180	Угроза отказа подсистемы обеспечения температурного режима	-	-	-	-	-
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	-	-	-	-	+
УБИ.182	Угроза физического устаревания аппаратных компонентов	-	-	-	-	+
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	+	+	+	+	+
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	-	-	-	-	+
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	+	+	+	+	+
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	-	-	-	+	+
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	+	+	+	+	+
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	-	-	-	+	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	+	+	+	+	+
УБИ.192	Угроза использования уязвимых версий программного обеспечения	+	+	+	+	+
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	+	+	+	+	+
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	-	-	-	-	+
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	-	-	-	-	+
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	-	-	-	-	+
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	-	-	-	-	+
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	+	+	-	-	+
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	-	-	-	-	+
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	-	-	-	-	+
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	-	-	-	-	+
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	-	-	-	-	+
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	-	-	-	-	+
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	-	-	-	-	+
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	+	+	-	-	+
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	-	-	-	-	+

Идентификатор УБИ	Наименование УБИ	Технологические (архитектурные) уровни				
		1	2	3	4	5
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	+	+	-	-	+
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	+	+	-	-	+
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	-	-	-	-	+
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	+	+	+	+	+
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечениям администрирования информационных систем	+	-	-	-	+
УБИ.212	Угроза перехвата управления информационной системой	+	+	+	+	+
УБИ.213	Угроза обхода многофакторной аутентификации	+	-	+	+	+
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.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	+	+	-	-	+
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	+	+	+	+	+
УБИ.218	Угроза раскрытия информации о модели машинного обучения	-	+	-	-	-
УБИ.219	Угроза хищения обучающих данных	-	+	-	-	-
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	-	+	-	-	-
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	-	+	-	-	-
УБИ.222	Угроза подмены модели машинного обучения	-	+	-	-	-

Пользователями ИС «АРМ-АИСТ» согласно настоящей Модели угроз должны рассматриваться угрозы безопасности информации следующих архитектурных уровней:

Уровень обеспечения прикладного ПО (2);

Уровень обеспечения АРМ (5).

Перечень внесенных изменений по структурно-функциональным характеристикам платформы.

По результатам рассмотрения актуальных видов нарушителей, структурно-функциональных характеристик, применяемых информационных технологий и особенностей функционирования ИС «АРМ-АИСТ» были внесены изменения в перечень угроз безопасности информации.

Перечень внесенных изменений в перечень угроз безопасности информации ИС «АРМ-АИСТ» с указанием обоснования приведен в таблице Таблица 12.

Таблица 12 – Перечень внесенных изменений в базовый перечень угроз безопасности информации ИС «АРМ-АИСТ»

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
Уровень обеспечения системного ПО				
	ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	Исключена	Разработчики системного ПО не рассматриваются в качестве потенциального нарушителя. В ИС «АРМ-ОГ» используется лицензионное системное ПО с открытым исходным кодом, уязвимости в котором регулярно устраняются производителем. В рамках технической поддержки системного ПО, осуществляемой в соответствии имеющихся лицензий на ПО или договорных обязательств, осуществляется регулярное обновление системного ПО. Внедрение недекларированных возможностей разработчиком влечет за собой высокие репутационные и финансовые риски для разработчика

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
	УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Исключена	Суперкомпьютеры не используются в информационной системе
	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Исключена	Беспроводные технологии не используются
	УБИ.107	Угроза отключения контрольных датчиков	Исключена	Контрольные датчики не используются в информационной системе
	УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Исключена	Оборудование с числовым программным управлением не используется
	УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Исключена	Суперкомпьютеры не используются
	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Исключена	Цифровая подпись кода в качестве связующей информации между программными компонентами системы и ее привилегиями не используется в информационной системе
	УБИ.169	Угроза наличия механизмов разработчика	Исключена	Производится выбор доверенных разработчиков, производителей и поставщиков
	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Исключена	Система реального времени не используется в информационной системе
	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Исключена	Автоматизированные системы управления технологическими процессами не используются
	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Исключена	Применение сторонних (не проверенных) дистрибутивов не осуществляется

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
	УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Исключена	Оборудование с ЧПУ не используется
	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Исключена	Используемое для администрирования программное обеспечение не использует конфигурационные файлы, сформированные на основе пользовательских данных
	УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Исключена	Устройства типа Smart-карт (Java Card) не используются
Уровень обеспечения прикладного ПО				
	ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	Исключена	Разработчики прикладного ПО не рассматриваются в качестве потенциального нарушителя. В ИС

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				«АРМ-ОГ» проводится комплекс приемочных испытаний по итогам разработки прикладного ПО. Оператор не является конкурентом производителей прикладного ПО, в ИС «АРМ-ОГ»» не обрабатывается информация, составляющая коммерческую тайну конкурентов производителей прикладного ПО. В особых случаях, в ИС «АРМ-ОГ» принимается решение о проведении контроля отсутствия недекларированных возможностей в прикладном ПО
	УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Исключена	Политика лицензирования использования программного обеспечения не основана на ограничении количества его установок или числа его пользователей
	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Исключена	Беспроводные технологии не используются
	УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Исключена	Оборудование с числовым программным управлением не используется
	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Исключена	Беспроводные технологии не используются
	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Исключена	Язык описания WSDL не используется
	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Исключена	Цифровая подпись кода в качестве связующей информации между

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				программными компонентами системы и ее привилегиями не используется в информационной системе
	УБИ.169	Угроза наличия механизмов разработчика	Исключена	Производится выбор доверенных разработчиков, производителей и поставщиков
	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Исключена	Системы реального времени не используются
	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Исключена	Автоматизированные системы управления технологическими процессами не используются
	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Исключена	Применение сторонних (не проверенных) дистрибутивов не осуществляется
	УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Исключена	Оборудование с ЧПУ не используется
	УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Исключена	Устройства типа Smart-карт (Java Card) не используются
Уровень обеспечения внутреннего сетевого взаимодействия				
	ДОП.003	Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	Исключена	Технические средства ИС «АРМ-ОГ» находятся в пределах контролируемых зон. Согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				государственную тайну, содержащейся в государственных информационных системах» защита обрабатываемой в государственных информационных системах информации от утечки по техническим каналам, отличным от визуального, не является обязательной
	ДОП.006	Угроза утечки акустической (речевой) информации	Исключена	Технические средства ИС «АРМ-ОГ» не располагаются в защищаемых помещениях, в которых циркулирует речевая информация ограниченного доступа. В ИС «АРМ-ОГ» отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами ИС «АРМ-ОГ»
	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Исключена	Беспроводные технологии не используются
	УБИ.041	Угроза межсайтового скриптинга	Исключена	Архитектура информационной системы не предполагает обращения к сторонним веб-сайтам с выполнением скриптовых сценариев на стороне системы
	УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Исключена	Политика лицензирования использования программного обеспечения не основана на ограничении количества его установок или числа его пользователей
	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Исключена	Беспроводные технологии не используются

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
	УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Исключена	АСУ ТП и ЧПУ не используются в информационной системе
	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Исключена	Беспроводные технологии не используются
	УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Исключена	Беспроводные технологии не используются
	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Исключена	Беспроводные технологии не используются
	УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Исключена	Суперкомпьютеры не используются
	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Исключена	Язык описания WSDL не используется
	УБИ.169	Угроза наличия механизмов разработчика	Исключена	Производится выбор доверенных разработчиков, производителей и поставщиков
	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Исключена	Системы реального времени не используются
	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Исключена	АСУ ТП и ЧПУ не используются в информационной системе
	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Исключена	Применение сторонних (не проверенных) дистрибутивов не осуществляется
Уровень обеспечения внешнего сетевого взаимодействия				
	ДОП.003	Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	Исключена	Технические средства ИС «АРМ-ОГ» находятся в пределах контролируемых зон.

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				Согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» защита обрабатываемой в государственных информационных системах информации от утечки по техническим каналам, отличным от визуального, не является обязательной
	ДОП.006	Угроза утечки акустической (речевой) информации	Исключена	Технические средства ИС «АРМ-ОГ» не располагаются в защищаемых помещениях, в которых циркулирует речевая информация ограниченного доступа. В ИС «АРМ-ОГ» отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами
	УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Исключена	Грид-системы не используются
	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Исключена	Беспроводные технологии не используются
	УБИ.041	Угроза межсайтового скриптинга	Исключена	Архитектура информационной системы не предполагает обращения к сторонним веб-сайтам с выполнением скриптовых сценариев на стороне системы
	УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Исключена	Грид-системы не используются

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
	УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Исключена	Политика лицензирования использования программного обеспечения не основана на ограничении количества его установок или числа его пользователей
	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Исключена	Беспроводные технологии не используются
	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Исключена	Беспроводные технологии не используются
	УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Исключена	Беспроводные технологии не используются
	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Исключена	Беспроводные технологии не используются
	УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Исключена	Суперкомпьютеры не используются
	УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Исключена	Грид-системы не используются
	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Исключена	Язык описания WSDL не используется
	УБИ.169	Угроза наличия механизмов разработчика	Исключена	Производится выбор доверенных разработчиков, производителей и поставщиков.
	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Исключена	Системы реального времени не используются
	УБИ.183	Угроза перехвата управления автоматизированной системой управления	Исключена	АСУ ТП и ЧПУ не используются в информационной системе

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
		технологическими процессами		
	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Исключена	Применение сторонних (не проверенных) дистрибутивов не осуществляется
Уровень обеспечения АРМ				
	ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	Исключена	Разработчики системного ПО не рассматриваются в качестве потенциального нарушителя. В ИС «АРМ-ОГ» используется лицензионное системное ПО с открытым исходным кодом, уязвимости в котором регулярно устраняются производителем. В рамках технической поддержки системного ПО, осуществляемой в соответствии имеющихся лицензий на ПО или договорных обязательств, осуществляется регулярное обновление системного ПО. Внедрение недекларированных возможностей разработчиком влечет за собой высокие репутационные и финансовые риски для разработчика
	ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	Исключена	Разработчики прикладного ПО не рассматриваются в качестве потенциального нарушителя. В ИС «АРМ-ОГ» проводится комплекс приемочных испытаний по итогам разработки прикладного ПО. Оператор не является конкурентом производителей прикладного ПО, в ИС «АРМ-ОГ» не обрабатывается информация,

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				составляющая коммерческую тайну конкурентов производителей прикладного ПО. В особых случаях, в ИС «АРМ-ОГ» принимается решение о проведении контроля отсутствия недекларированных возможностей в прикладном ПО
	ДОП.003	Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	Исключена	Технические средства ИС «АРМ-ОГ» находятся в пределах контролируемых зон. Согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» защита обрабатываемой в государственных информационных системах информации от утечки по техническим каналам, отличным от визуального, не является обязательной
	ДОП.006	Угроза утечки акустической (речевой) информации	Исключена	Технические средства ИС «АРМ-ОГ» не располагаются в защищаемых помещениях, в которых циркулирует речевая информация ограниченного доступа. В ИС «АРМ-ОГ» отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Исключена	Беспроводные технологии не используются
	УБИ.041	Угроза межсайтового скриптинга	Исключена	Архитектура информационной системы не предполагает обращения к сторонним веб-сайтам с выполнением скриптовых сценариев на стороне системы
	УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Исключена	Политика лицензирования использования программного обеспечения не основана на ограничении количества его установок или числа его пользователей
	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Исключена	Беспроводные технологии не используются
	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Исключена	Беспроводные технологии не используются
	УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Исключена	Беспроводные технологии не используются
	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Исключена	Беспроводные технологии не используются
	УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Исключена	Суперкомпьютеры не используются
	УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Исключена	Грид-системы не используются в информационной системе
	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Исключена	Язык описания WSDL не используется
	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Исключена	Цифровая подпись кода в качестве связующей информации между программными компонентами системы и

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
				ее привилегиями не используется в информационной системе
	УБИ.169	Угроза наличия механизмов разработчика	Исключена	Производится выбор доверенных разработчиков, производителей и поставщиков.
	УБИ.172	Угроза распространения «почтовых червей»	Исключена	Системы электронных писем в информационной системе не используются
	УБИ.173	Угроза «спама» веб-сервера	Исключена	В информационной системе отсутствует объект воздействия имеющий функционал для реализации угрозы
	УБИ.174	Угроза «фарминга»	Исключена	Архитектура информационной системы не предполагает публично опубликованных веб-сайтов на которых требуется ввод защищаемой информации
	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Исключена	Системы реального времени не используются
	УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Исключена	Система реального времени не используется в информационной системе
	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Исключена	Автоматизированные системы управления технологическими процессами не используются
	УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.191	Угроза внедрения вредоносного кода в	Исключена	Применение сторонних (не проверенных)

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
		дистрибутив программного обеспечения		дистрибутивов не осуществляется
	УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Исключена	В составе технических средств ИС «АРМ-ОГ» и технических средств внутренних пользователей ИС «АРМ-ОГ» отсутствуют мобильные технические средства
	УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Исключена	Неподключенные к сети Интернет технические средства в составе ИС «АРМ-ОГ» не используются.
	УБИ.204	Угроза несанкционированного изменения	Исключена	Автоматизированные системы

№ п/п	Идентификатор УБИ	Наименование УБИ	Изменение	Обоснование
		вредоносной программой значений параметров программируемых логических контроллеров		управления технологическими процессами не используются
	УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Исключена	Оборудование с ЧПУ не используется
	УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Исключена	Оборудование с ЧПУ не используется
	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Исключена	Используемое для администрирования программное обеспечение не использует конфигурационные файлы, сформированные на основе пользовательских данных
	УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Исключена	Устройства типа Smart-карт (Java Card) не используются

12. Адаптированный перечень угроз безопасности информации платформы

Адаптированный таким образом перечень рассматриваемых угроз безопасности информации ИС «АРМ-АИСТ» приведен в таблице Таблица 2.

Таблица 12 – Адаптированный перечень угроз безопасности информации ЦП «ГосТех»

Идентификатор УБИ	Наименование УБИ
Уровень обеспечения системного ПО	
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления аутентификационной информации
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов 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.033	Угроза использования слабостей кодирования входных данных
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.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия

Идентификатор УБИ	Наименование УБИ
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.056	Угроза некачественного переноса инфраструктуры в облако
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.063	Угроза некорректного использования функционала программного обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
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.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.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры

Идентификатор УБИ	Наименование УБИ
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.101	Угроза общедоступности облачной инфраструктуры
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.109	Угроза перебора всех настроек и параметров приложения
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.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
УБИ.137	Угроза потери управления облачными ресурсами
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных

Идентификатор УБИ	Наименование УБИ
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.158	Угроза форматирования носителей информации
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.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
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.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.189	Угроза маскирования действий вредоносного кода
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
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

Идентификатор УБИ	Наименование УБИ
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.212	Угроза перехвата управления информационной системой
УБИ.213	Угроза обхода многофакторной аутентификации
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
Уровень обеспечения прикладного ПО	
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления аутентификационной информации
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
УБИ.023	Угроза изменения компонентов 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.033	Угроза использования слабостей кодирования входных данных
УБИ.036	Угроза исследования механизмов работы программы

Идентификатор УБИ	Наименование УБИ
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного обеспечения
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных

Идентификатор УБИ	Наименование УБИ
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.122	Угроза повышения привилегий
УБИ.127	Угроза подмены действия пользователя путём обмана
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.132	Угроза получения предварительной информации об объекте защиты
УБИ.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.159	Угроза «форсированного веб-браузинга»

Идентификатор УБИ	Наименование УБИ
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
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.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
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
УБИ.218	Угроза раскрытия информации о модели машинного обучения
УБИ.219	Угроза хищения обучающих данных
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных
УБИ.222	Угроза подмены модели машинного обучения

Идентификатор УБИ	Наименование УБИ
Уровень обеспечения внутреннего сетевого взаимодействия	
ДОП.004	Природные угрозы
ДОП.005	Техногенные угрозы
УБИ.005	Угроза внедрения вредоносного кода в BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления 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.017	Угроза доступа/перехвата/изменения HTTP cookies
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.023	Угроза изменения компонентов системы
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.026	Угроза искажения XML-схемы
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 УБИ	Наименование УБИ
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.055	Угроза незащищённого администрирования облачных услуг
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных
УБИ.063	Угроза некорректного использования функционала программного обеспечения
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи
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.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети

Идентификатор УБИ	Наименование УБИ
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему 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.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.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS

Идентификатор УБИ	Наименование УБИ
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.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
УБИ.137	Угроза потери управления облачными ресурсами
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев
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.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
УБИ.150	Угроза сбоя процесса обновления BIOS
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.165	Угроза включения в проект не достоверно испытанных компонентов

Идентификатор УБИ	Наименование УБИ
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.189	Угроза маскирования действий вредоносного кода
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.212	Угроза перехвата управления информационной системой
УБИ.213	Угроза обхода многофакторной аутентификации
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
Уровень обеспечения внешнего сетевого взаимодействия	
ДОП.004	Природные угрозы
ДОП.005	Техногенные угрозы
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.005	Угроза внедрения вредоносного кода в BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления аутентификационной информации

Идентификатор УБИ	Наименование УБИ
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.016	Угроза доступа к локальным файлам сервера при помощи URL
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.023	Угроза изменения компонентов системы
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.026	Угроза искажения XML-схемы
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
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS

Идентификатор УБИ	Наименование УБИ
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.055	Угроза незащищённого администрирования облачных услуг
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.063	Угроза некорректного использования функционала программного обеспечения
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи
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.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб

Идентификатор УБИ	Наименование УБИ
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.114	Угроза переполнения целочисленных переменных
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
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.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
УБИ.137	Угроза потери управления облачными ресурсами

Идентификатор УБИ	Наименование УБИ
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев
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.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
УБИ.150	Угроза сбоя процесса обновления BIOS
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.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.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.175	Угроза «фишинга»
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.189	Угроза маскирования действий вредоносного кода

Идентификатор УБИ	Наименование УБИ
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.212	Угроза перехвата управления информационной системой
УБИ.213	Угроза обхода многофакторной аутентификации
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
7. ТК АРМ. Уровень обеспечения АРМ	
ДОП.004	Природные угрозы
ДОП.005	Техногенные угрозы
ДОП.007	Угроза утечки видовой информации
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.005	Угроза внедрения вредоносного кода в BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления 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

Идентификатор УБИ	Наименование УБИ
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
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 системы
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.026	Угроза искажения XML-схемы
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
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS

Идентификатор УБИ	Наименование УБИ
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.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.055	Угроза незащищённого администрирования облачных услуг
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 обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
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.075	Угроза несанкционированного доступа к виртуальным каналам передачи
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.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.093	Угроза несанкционированного управления буфером

Идентификатор УБИ	Наименование УБИ
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему 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.120	Угроза перехвата управления средой виртуализации
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

Идентификатор УБИ	Наименование УБИ
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.132	Угроза получения предварительной информации об объекте защиты
УБИ.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
УБИ.137	Угроза потери управления облачными ресурсами
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.139	Угроза преодоления физической защиты
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев
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.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.152	Угроза удаления аутентификационной информации
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»

Идентификатор УБИ	Наименование УБИ
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
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.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.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
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.192	Угроза использования уязвимых версий программного обеспечения

Идентификатор УБИ	Наименование УБИ
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
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.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.212	Угроза перехвата управления информационной системой
УБИ.213	Угроза обхода многофакторной аутентификации
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

13. Заключение

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 для ИСПДн «АРМ-АИСТ» на базе автоматизированного рабочего места администрации Первомайского района Тамбовской области актуальны угрозы 3-го типа (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн).

В соответствии с приказом ФСБ России 10 июля 2014 г. № 378 «Об утверждении состава и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» в ИСПДн для нейтрализации атак необходимо использовать СКЗИ класса КС2.