Министерство энергетики Российской Федерации
(МИНЭНЕРГО РОССИИ)

МИНИСТР

ул. Щепкина, д. 42, стр. 1, стр. 2, г. Москва,
ГСП-6, 107996
Тел. (495) 631-98-58, Факс (495) 631-83-64
E-mail: minenergo@minenergo.gov.ru
http://www.minenergo.gov.ru

29.06.2021 № НШ-7491/07

На № _____ от _____

Руководителям сетевых организаций и гарантирующих поставщиков

О базовой модели угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности)

Уважаемые коллеги!

Во исполнение абзаца четвертого пункта 2 постановления Правительства Российской Федерации от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)» Министерством энергетики Российской Федерации совместно с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации разработана базовая модель угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности) (прилагается).

Базовая модель угроз безопасности информации подлежит пересмотру в срок до 31 декабря 2023 г. в части использования в приборах учета электрической энергии средств криптографической защиты информации, сертифицированных ФСБ России.

Приложение: на 60 л. в 1 экз.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат E1036E1B07E00081EB11212411DB06B7
Владелец Шульгинов Николай Григорьевич
Действителен с 11.11.2020 по 11.11.2021

Н.Г. Шульгинов

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИВК – информационно-вычислительный комплекс

ИВКЭ – информационно-вычислительный комплекс электроустановки

ИСУЭ – интеллектуальная система учета электрической энергии (мощности)

ИТС – информационно-телекоммуникационная сеть

ПУ – прибор учета электрической энергии

КИИ – критическая информационная инфраструктура Российской Федерации

НСД – несанкционированный доступ

УБИ – угрозы безопасности информации

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

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

Владелец интеллектуальной системы учета электрической энергии (мощности) – сетевая организация и (или) гарантирующий поставщик, обеспечивающий безвозмездное предоставление возможности использования функций интеллектуальной системы учета электрической энергии (мощности) в порядке, установленном Правилами доступа к минимальному набору функций интеллектуального учета электрической энергии (мощности), утвержденных постановлением Правительства Российской Федерации от 19.06.2020 № 890, субъектам электроэнергетики и потребителям электрической энергии, в отношении которых они обеспечивают коммерческий учет электрической энергии.

Доступ к информации – возможность получения информации и ее использования.

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

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование,

предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

Интеллектуальная система учета электрической энергии (мощности) - совокупность функционально объединенных компонентов и устройств, предназначенная для удаленного сбора, обработки, передачи показаний приборов учета электрической энергии, обеспечивающая информационный обмен, хранение показаний приборов учета электрической энергии, удаленное управление ее компонентами, устройствами и приборами учета электрической энергии, не влияющее на результаты измерений, выполняемых приборами учета электрической энергии, а также предоставление информации о результатах измерений, данных о количестве и иных параметрах электрической энергии в соответствии с правилами предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности), утвержденными Правительством Российской Федерации.

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.

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

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.

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

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

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Оператор – юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации

физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

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

Технические средства – технические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

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

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

НОРМАТИВНЫЕ ССЫЛКИ

В настоящем документе использованы нормативные ссылки на следующие документы:

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике»;

– постановление Правительства Российской Федерации от 19.06.2020 № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)»;

– постановление Правительства РФ от 06.07.2015 N 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

– приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденная Заместителем директора ФСТЭК России 18.05.2007;

– «Базовая модель угроз безопасности персональных данных при обработке в информационной системе персональных данных», утвержденная Заместителем директора ФСТЭК России 15.02.2008.

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая «Базовая модель угроз безопасности информации интеллектуальной системы учёта электрической энергии (мощности)» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности информации, влияющих на обеспечение устойчивого функционирования интеллектуальной системы учета электрической энергии (мощности) (далее – ИСУЭ) в проектных режимах работы и безопасность обрабатываемых персональных данных при проведении в отношении неё компьютерных атак.

Модель угроз содержит исходные данные по угрозам безопасности информации в ИСУЭ, связанным:

– с воздействием на метрологические характеристики компонентов ИСУЭ;

– с воздействием на компоненты ИСУЭ в целях управления подачей электрической энергии (мощности) потребителю;

– с воздействие на компоненты ИСУЭ в целях нарушения их функционирования в проектных режимах работы;

– с несанкционированным доступом к компонентам ИСУЭ с целью деструктивного воздействия на обрабатываемые в них персональные данные.

Модель угроз является методическим документом для подразделений (работников) субъектов критической информационной инфраструктуры Российской Федерации, ответственных за обеспечение безопасности объектов критической информационной инфраструктуры Российской Федерации, руководителей субъектов критической инфраструктуры Российской Федерации, организующих и проводящих мероприятия по реализации мер по обеспечению безопасности информации.

Модель угроз содержит краткое описание ИСУЭ и базовый перечень актуальных угроз безопасности информации.

Угрозы безопасности информации, содержащиеся в Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности информации, изменений архитектуры и функциональности ИСУЭ.

Владельцы ИСУЭ, которым на праве собственности, аренды или ином законном основании принадлежат объекты критической информационной инфраструктуры, обязаны определять угрозы безопасности информации и разрабатывать на их основе модели угроз безопасности информации с учетом положений Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также обеспечивать непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

При разработке частной модели угроз безопасности информации, угрозы в отношении информационно-вычислительного комплекса, информационно-вычислительного комплекса электроустановки и прибора учета электрической энергии, установленные настоящим документом, могут быть пересмотрены владельцем ИСУЭ, в случае их неприменимости к используемым технологиям обработки информации.

Пересмотр состава угроз безопасности информации должен осуществляться, как минимум, в следующих случаях:

– изменения требований законодательства Российской Федерации в области защиты информации и методических документов, раскрывающих вопросы защиты информации;

– изменения условий и особенностей функционирования и эксплуатации ИСУЭ, следствием которых стало возникновение новых угроз безопасности информации;

– выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

– появления сведений и фактов о новых возможностях нарушителей.

Угрозы, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, сертифицированных ФСБ России (далее – СКЗИ), определяются для каждого конкретного информационно-вычислительного комплекса в зависимости от наличия объектов критической информационной инфраструктуры, подключаемых к ней, а также от необходимости обработки информации, подлежащей защите в соответствии с законодательством Российской Федерации.

Для систем и их компонентов, которые в соответствии с Моделью угроз требуют применения СКЗИ должна разрабатываться частная модель угроз безопасности информации в отношении СКЗИ.

В случае нарушений установленной законодательством Российской Федерации длительности перерывов электроснабжения и (или) предоставления услуг по передаче электрической энергии в результате реализации угроз безопасности информации, владелец интеллектуальной системы учета электрической энергии (мощности) возмещает ущерб, причиненный потребителям электрической энергии вследствие реализации угроз безопасности информации, в порядке и размере, определенных законодательством Российской Федерации.

В частной модели угроз безопасности в отношении СКЗИ к объектам защиты должны быть отнесены СКЗИ, среда функционирования СКЗИ и данные, обмен которыми осуществляется между информационно-вычислительным комплексом и прибором учета электрической энергии и между информационно-вычислительным комплексом и информационно-вычислительным комплексом электроустановки в соответствии с требованиями постановления Правительства Российской Федерации от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)».

В случае принятия решения об обеспечении некорректируемой регистрации информации в ИСУЭ криптографическими методами, разработка шифровальных (криптографических) средств, реализующих указанные методы, должна осуществляться в соответствии с «Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66, с учетом «Требований к средствам криптографической информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну».

ОПИСАНИЕ СТРУКТУРНО-ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТРИК ИСУЭ

Общие сведения

ИСУЭ построена по клиент-серверной архитектуре и может иметь в соответствии с выполняемыми функциями три функциональных уровня, объединённых между собой посредством применения различных средств и каналов связи. Функциональными уровнями являются:

информационно-вычислительный комплекс (далее – ИВК) – находящаяся на верхнем уровне ИСУЭ совокупность функционально объединённых программных и технических средств для решения задач сбора, хранения, передачи и обработки данных учета электрической энергии и сопутствующей информации, удаленного управления компонентами системы учета электрической энергии и нагрузкой;

информационно-вычислительный комплекс электроустановки (далее – ИВКЭ) – находящиеся на среднем уровне ИСУЭ совокупность программных и технических средств для решения задач сбора, хранения, передачи в ИВК и обработки данных учета электрической энергии и сопутствующей информации, удаленного управления приборами учета электрической энергии и их нагрузкой;

приборы учета электрической энергии (далее – ПУ) – находящиеся на нижнем уровне ИСУЭ средства измерения, представляющие собой представляет собой программно-аппаратные средства, допущенные в эксплуатацию для целей коммерческого учета электрической энергии на розничных рынках электрической энергии и (или) предоставления коммунальных услуг по электроснабжению и присоединенный к ИСУЭ, и соответствующие требованиям Правил доступа к минимальному набору функций интеллектуального учета электрической энергии (мощности), утвержденных постановлением Правительства Российской Федерации

от 19.06.2020 № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)» (далее – Правила доступа).

Пример двухуровневой и трехуровневой общей структурно-коммуникационной схемы ИСУЭ представлена на рисунке 1.

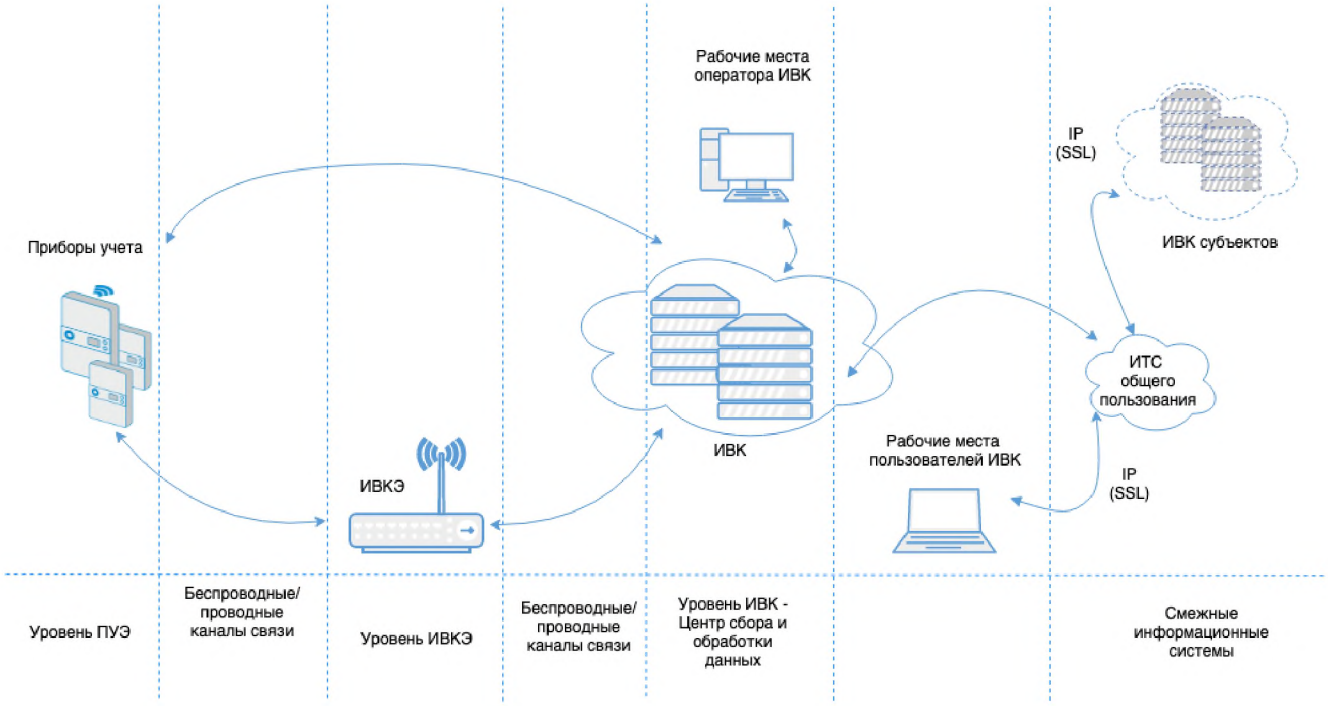

Рисунок 1. Пример общей структурно-коммуникационной схемы ИСУЭ и ПУ

ИВК предназначен для:

– дистанционного считывания, накопления, обработки, хранения и отображения результатов измерений, количества и иных параметров электрической энергии, журналов событий и данных о параметрах настройки ИВКЭ и ПУ по протоколам обмена данными;

– управления ПУ, присоединенными к ИВК как непосредственно (двухуровневая схема), так и опосредованно через ИВКЭ (трехуровневая схема);

– изменения конфигурационных параметров ИВКЭ и ПУ, а также для обновления программного обеспечения.

ИВКЭ предназначен для:

– дистанционного считывания, накопления, обработки, хранения и отображения результатов измерений, количества и иных параметров электрической энергии, журналов событий и данных о параметрах настройки ПУ по протоколам обмена данными;

– управления ПУ, присоединенными к ИВКЭ;

– изменения конфигурационных параметров ПУ, а также для обновления программного обеспечения.

В ИВК, ИВКЭ и ПУ обеспечивается многопользовательский режим обработки информации, в том числе путем предоставления доступа по информационно-телекоммуникационной сети общего пользования.

В ИСУЭ на уровне ИВК в случае наличия такой потребности могут обрабатываться персональные данные.

Эксплуатация оборудования ИВК выполняется в пределах границ контролируемой зоны. ИВКЭ и ПУ могут размещаться вне границ контролируемой зоны.

В зависимости от условий эксплуатации программные и технические элементы ИВК могут быть территориально распределены по различным центрам сбора и обработки данных.

В зависимости от условий эксплуатации и наличия такой потребности ИВК могут взаимодействовать с различными смежными системами.

Информационное взаимодействие компонентов и устройств ИСУЭ обеспечивается между:

ИВК и ИВКЭ/ПУ - по проводным и беспроводным каналам связи;

ИВКЭ и ПУ – по проводным, беспроводным каналам связи и линиям электропередачи.

Технологическое обслуживание (настройка) ИВКЭ и ПУ обеспечивается операторами по каналам связи или подключением непосредственно к внешнему цифровому интерфейсу связи комплекса.

Коммутационным оборудованием, входящим в состав ИВКЭ, обеспечивается реализация процесса по созданию логического соединения

между ИВК и ПУ за счет инкапсулирования протоколов обмена данными ИВК и ПУ для организации прямого соединения между ними.

Обмен данными между ПУ и ИВК/ИВКЭ построен по клиент-серверной архитектуре, в соответствии с которой ПУ выполняет роль сервера, а ИВК/ИВКЭ - роль клиента. В рамках данной архитектуры ИВКЭ или ИВК выступают инициатором обмена данными при опросе ПУ.

Информационный обмен в ИСУЭ может осуществляется как в пределах одного уровня (между одноранговыми устройствами), так и между уровнями.

Сеть передачи информации ИСУЭ может строится как на собственных (ведомственных), так и на арендованных каналах связи (в том числе операторов сотовой связи).

Присоединенные к ИСУЭ ПУ, могут передавать информацию по проводным и (или) беспроводным сетям связи, а также по линиям электропередачи с применением соответствующих технологий.

Технические средства ИСУЭ имеют возможность локального и дистанционного доступа и управления.

В случае деструктивного воздействия на ПУ (например, вскрытие клеммной крышки, воздействия магнитным полем, попытках несанкционированного доступа, изменения интерфейсного программного обеспечения, при превышении максимальной мощности, при отклонении от нормированного значения уровня напряжения и т.п.) ПУ выступает инициатором передачи данных деструктивного воздействия на верхний уровень (ИВК или ИВКЭ).

В соответствие с Правилами доступа, в функции ПУ входит осуществление полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии, приостановление или ограничение предоставления коммунальной услуги (управление нагрузкой) с использованием встроенного коммутационного аппарата (кроме ПУ

трансформаторного включения). Указанные ограничения осуществляются в следующих случаях:

– запрос от ИВК;

– превышение заданных в ПУ пределов параметров электрической сети;

– превышение заданного в ПУ предела электрической энергии (мощности);

– несанкционированный доступ к ПУ (например, вскрытие клеммной крышки, вскрытие корпуса (для разборных корпусов) и воздействие постоянным и переменным магнитным полем).

В соответствии с Правилами доступа восстановление функций ПУ в случаях их отказа должно быть обеспечено в течение 7 дней со дня обнаружения отказа владельцем ИСУЭ или получения сообщения от пользователя ИСУЭ.

В случае возникновения необходимости проведения восстановительных работ владелец ИСУЭ в срок, не превышающий 2 часов с момента возобновления доступа к минимальным функциям ИСУЭ, обязан довести такую информацию до пользователей ИСУЭ путем размещения на своем официальном сайте в информационно-телекоммуникационной сети «Интернет» (применения иного способа информирования) объявления, которое должно содержать причину, дату и время прекращения доступа, а также дату и время возобновления доступа к минимальному набору функций ИСУЭ, при этом продолжительность таких работ не должна превышать 72 часов в месяц.

ФУНКЦИОНАЛ ИВК

Наиболее значимыми для моделирования угроз являются следующие основные функции ИВК:

– сбор и обработка показаний и результатов измерений ПУ;

– предоставление информации о количестве и иных параметрах электрической энергии;

– полное и (или) частичное ограничение режима потребления электрической энергии (приостановление или ограничение предоставления коммунальной услуги), а также возобновление подачи электрической энергии;

– установление и изменение зон суток (часов, дней недели, месяцев), по которым ПУ осуществляется суммирование объемов электрической энергии в соответствии с дифференциацией тарифов (цен), предусмотренной законодательством Российской Федерации;

– обработка событий и оповещение потребителя о возможных недостоверных данных, поступающих с приборов учета в случае срабатывания индикаторов вскрытия электронных пломб на корпусе и клеммной крышке ПУ, воздействия магнитным полем на элементы прибора учета, неработоспособности ПУ вследствие аппаратного или программного сбоя, его отключения (после повторного включения), перезагрузки;

– синхронизация времени как самого устройства, так и в подключаемых ПУ.

Дополнительно ИВК должен обеспечивать выполнение функций управления параметрами конфигурационной настройки ИВКЭ и ПУ, в том числе обновлению их программного обеспечения по защищенным протоколам обмена данными.

Наиболее значимой для моделирования угроз является передача ИВК следующей информации:

– результаты измерений, количества и иных параметров электрической энергии (мощности) ПУ;

– параметры профилей загрузки, времени, профилей телеизмерений и телесигнализации, обслуживаемых ПУ;

– параметры идентификации (аутентификации) ПУ (уникальных логических имен);

– события ПУ и ИВКЭ, связанные с током, напряжением, коммутацией реле нагрузки ПУ, программирования параметров ПУ, внешним воздействием, с коммуникационными событиями, с контролем доступа, и других событий).

Архитектура ИВК, в том числе комплекс серверного и телекоммуникационного оборудования, состав системного и прикладного программного обеспечения, протоколы обмена данными со смежными информационными системами должны определяться нормативно-техническими документами и стандартами субъектов.

ФУНКЦИОНАЛ ИВКЭ

Наиболее значимыми для моделирования угроз являются следующие основные функции ИВКЭ:

– сбор, обработка данных ПУ и их передачу в ИВК (показаний и результатов измерений, информации о количестве и иных параметрах электрической энергии, о параметрах настройки и событиях, справочной информации, архива данных);

– изменение параметров конфигурации ПУ;

– трансляция команды на полное и (или) частичное ограничение режима потребления электрической энергии (приостановление или ограничение предоставления коммунальной услуги), а также возобновление подачи электрической энергии;

– установление и изменение зон суток (часов, дней недели, месяцев), по которым ПУ осуществляется суммирование объемов электрической энергии в соответствии с дифференциацией тарифов (цен), предусмотренной законодательством Российской Федерации;

– оповещение о возможных недостоверных данных, поступающих с ПУ в случае срабатывания индикаторов вскрытия электронных пломб на корпусе и клеммной крышке ПУ, воздействия магнитным полем на элементы ПУ, неработоспособности ПУ вследствие аппаратного или программного сбоя, его отключения (после повторного включения), перезагрузки;

– синхронизация времени как самого устройства, так и в подключаемых ПУ.

Наиболее значимой для моделирования угроз является передача ИВКЭ следующей информации:

– результаты измерений, количества и иных параметров электрической энергии (мощности) ПУ;

– параметры профилей загрузки, времени ПУ;

– параметры идентификации (аутентификации) (уникальных логических имен), в том числе ПУ;

– события ПУ, связанные с изменением тока, напряжения, коммутацией реле нагрузки ПУ, программирования параметров ПУ, коммуникационными событиями, с контролем доступа;

– события ИВКЭ, связанные с программированием параметров, коммуникационными событиями и контролем доступа);

– параметры сетевой настройки устройств связи ПУ и ИВКЭ.

В соответствии с пунктом 37 Правил доступа, количество ПУ с функцией полного и (или) частичного ограничения режима потребления электрической энергии, приостановления или ограничения предоставления коммунальной услуги (управление нагрузкой), контролируемых ИВКЭ, не должно превышать 750 ПУ (точек поставки, лицевых счетов - в отношении многоквартирных домов, договоров, содержащих положения о предоставлении коммунальной услуги по электроснабжению).

ФУНКЦИОНАЛ ПУ

Функционал ПУ изложен в пункте 28 Правил доступа.

Наиболее значимыми для моделирования угроз являются следующие функции ПУ:

– измерение и расчет в режиме реального времени (активной и реактивной энергии, фазного напряжения, тока (пофазного), тока в нулевом проводе, активной, реактивной и полной мощности, соотношение активной и реактивной мощности, частоты сети, небаланса токов в фазном и нулевом проводах);

– измерение индивидуальных показателей качества электроэнергии;

– фиксация измерений по времени;

– ограничение потребления и мощности;

– наличие «Журнала событий»;

– наличие автоматической самодиагностики с формированием обобщённого сигнала в «Журнале событий».

Наиболее значимой для моделирования угроз является передача следующей информации ПУ:

– результаты измерений, количества и иных параметров электрической энергии (мощности);

– параметры профиля загрузки, времени;

– управляющая (командная) информация;

– параметры идентификации (аутентификации) (уникальное логическое имя);

– события, связанные с током, напряжением, включение/выключением ПУ, программирования параметров ПУ, внешним воздействием, с коммуникационными событиями, с контролем доступа);

– параметры сетевой настройки устройств связи.

Предусмотрена следующая классификация индивидуальных и общих (квартирных) ПУ жилых домов (домовладений) и ПУ объектов энергопринимающих устройств, принадлежащих юридическим лицам, присоединяемых к ИСУЭ:

– однофазный;

– трехфазный непосредственного (прямого) подключения;

– трехфазный трансформаторного подключения с использованием измерительных трансформаторов тока (полукосвенного подключения);

– трехфазный трансформаторного подключения с использованием измерительных трансформаторов тока и напряжения (косвенного подключения).

Встроенное реле управления нагрузкой имеется только у однофазных и трехфазных приборов учета электроэнергии непосредственного (прямого) подключения, обладающих функциональностью полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии, приостановление или ограничение предоставления коммунальной услуги (управление нагрузкой) с использованием встроенного коммутационного аппарата, в том числе путем его фиксации в положении "отключено" непосредственно на приборе учета электрической энергии, в следующих случаях:

– запрос интеллектуальной системы учета;

– превышение заданных в ПУ пределов параметров электрической сети;

– превышение заданного в ПУ предела электрической энергии (мощности);

– несанкционированный доступ к ПУ (вскрытие клеммной крышки, вскрытие корпуса (для разборных корпусов) и воздействие постоянным и переменным магнитным полем).

КЛАССИФИКАЦИЯ
УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

По виду информации, на которую направлены угрозы:		
Угрозы видовой информации	Угрозы информации, обрабатываемой в технических средствах ИСУЭ	Угрозы информации, обрабатываемой в АРМ операторов ИСУЭ

По виду нарушаемого свойства информации:		
Угрозы доступности (нарушения функционирования в проектных режимах работы)	Угрозы целостности (утраты, уничтожения, модификации) информации	Угрозы конфиденциальности (утечки, перехвата, съема, копирования, хищения информации, а также деструктивных воздействий на обрабатываемые в ИСУЭ персональные данные)

По типовым объектам информации, для которых угрозы представляют опасность:			
Угрозы ИВК	Угрозы ИВКЭ	Угрозы ПУ	Угрозы направленные на каналы связи межу ИВК, ИВКЭ, ПУ

По видам возможных источников угроз:		
Создаваемые нарушителем: внутренним с низким потенциалом, внутренним со средним потенциалом, внутренним с высоким потенциалом, внешним с низким потенциалом, внешним со средним потенциалом, внешним с высоким потенциалом	Создаваемые аппаратной закладкой, встроенная закладка, автономная закладка	Реализуемые с помощью вредоносных программ (вирусов)

По используемой уязвимости:				
В микропрограммном, общесистемном, прикладном программном обеспечение	С использованием аппаратной закладки	С используемыми протоколами передачи данных	Уязвимости связанные с недостатками организации технической защиты информации от НСД	С использованием уязвимостей СЗИ

По объектам воздействия:						
Аппаратное обеспечение (в том числе	виртуальная машина, виртуальные	рабочая станция, средство защиты информации,	Каналы связи (передачи) данных, сетевой трафик,	Информация, хранящаяся на компьютере во временных файлах,	Носители информации	Микропрограммное обеспечение (в том числе BIOS/UEFI),

BIOS/UEFI), аппаратное средство, аппаратное устройство	устройства хранения данных, виртуальные диски, гипервизор	информационная система, инфраструктура информационных систем, сервер	сетевой узел, телекоммуникационное устройство	объекты файловой системы, аутентификационные данные пользователя (программное обеспечение), реестр		прикладное программное обеспечение, программное обеспечение, системное программное обеспечение, сетевое программное обеспечение

По способам реализации угроз безопасности:
Угрозы, связанные с НСД (в том числе, компьютерные атаки) к типовым объектам информации.

Рисунок 2. Классификация угроз безопасности.

МОДЕЛЬ НАРУШИТЕЛЯ ИСУЭ

С учетом наличия прав доступа и возможностей по доступу к информации, обрабатываемой в ИСУЭ, нарушители подразделяются на два типа:

- внешние нарушители – субъекты, не имеющие прав (полномочий) по доступу к информационным ресурсам и компонентам ИСУЭ;

- внутренние нарушители – субъекты, имеющие права (полномочия) по доступу к информационным ресурсам и компонентам ИСУЭ.

В соответствии с банком данных угроз ФСТЭК России определяется три типа внешних и внутренних нарушителей – с низким потенциалом, средним потенциалом и высоким потенциалом.

Нарушители с низким потенциалом имеют возможность получить информацию об уязвимостях основных компонентов ИСУЭ, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак на основные компоненты ИСУЭ.

Нарушители со средним потенциалом обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в основных компонентах ИСУЭ. Имеют возможность получить информацию об уязвимостях основных компонентов ИСУЭ путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения, установленного на основных компонентах ИСУЭ. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования основных компонентов ИСУЭ.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам основных компонентов ИСУЭ для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в основных компонентах ИСУЭ, об алгоритмах, аппаратных и программных средствах, используемых в основных компонентах ИСУЭ. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств. Имеют возможность создания и применения специальных технических средств для добывания информации.

С учетом типов нарушителей по видам нарушители безопасности информации подразделяются на 11 видов, приведенных в таблице 1.

Таблица 1

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация)реализации угроз безопасности информации	Потенциал нарушителя

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация)реализации угроз безопасности информации	Потенциал нарушителя
1	Специальные службы иностранных государств (блоков государств)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций	Высокий (на всех уровнях)
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций	Средний (на всех уровнях)
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Средний (на всех уровнях)
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Низкий (на всех уровнях)
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием	Средний (на всех уровнях)
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные,	Средний (на всех уровнях)

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация)реализации угроз безопасности информации	Потенциал нарушителя
			неосторожные или неквалифицированные действия	
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Средний (на всех уровнях)
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру (администрация, охрана, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Средний (на всех уровнях)
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Низкий (на всех уровнях)
10	Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Высокий (на всех уровнях)
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.	Средний (на всех уровнях)

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ИВК

При обработке информации на уровне ИВК возможна реализация следующих угроз безопасности информации (далее – УБИ):

угрозы информации, обрабатываемой в технических средствах ИВК;

угрозы информации, обрабатываемой в АРМ операторов ИВК;

угрозы утечки видовой информации;

угрозы преднамеренного искажения системного времени в компонентах ИСУЭ.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИВК.

Угрозы НСД в ИВК связаны с действиями нарушителей, имеющих доступ к ИВК, включая операторов АРМ, реализующих угрозы непосредственно в ИВК. Кроме этого, источниками угроз НСД к информации в ИВК могут быть нарушители с различным потенциалом, а также аппаратные закладки и вредоносные программы.

В ИВК возможны все виды уязвимостей в том числе: уязвимости в микропрограммном, общесистемном, прикладном программном обеспечение, уязвимости, связанные с используемыми протоколами передачи данных, уязвимости, в связи с возможностью наличия аппаратных закладок, уязвимости связанные с недостатками организации ТЗИ от НСД, уязвимости в СЗИ.

В ИВК в соответствии с используемыми технологиями, объектами воздействия, уязвимостями возможны следующие угрозы из Банка данных угроз безопасности информации ФСТЭК России:

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 и/или повторного использования аутентификационной информации;

УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS;

УБИ.010: Угроза выхода процесса за пределы виртуальной машины;

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.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 информационной; (автоматизированной) 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 дентификации/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.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS;

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;

УБИ.048: Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

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. 053: Угроза невозможности управления правами пользователей BIOS;

УБИ.058: Угроза неконтролируемого роста числа виртуальных машин;

УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;

УБИ.061: Угроза некорректного задания структуры данных транзакции;

УБИ.063: Угроза некорректного использования функционала программного и аппаратного обеспечения;

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

УБИ.069[1]: Угроза неправомерных действий в каналах связи;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;

УБИ.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;

---

[1] Угроза нейтрализуется с помощью СКЗИ на канале связи между ИВК и ИВКЭ.

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.083[2]: Угроза несанкционированного доступа к системе по беспроводным каналам;

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;

---

[2] Угроза нейтрализуется с помощью СКЗИ на канале связи между ИВК и ИВКЭ.

УБИ.095: Угроза несанкционированного управления указателями;

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

УБИ.099: Угроза обнаружения хостов;

УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации;

УБИ.102: Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ.103: Угроза определения типов объектов защиты;

УБИ.104: Угроза определения топологии вычислительной сети;

УБИ.108: Угроза ошибки обновления гипервизора;

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.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.127: Угроза подмены действия пользователя путём обмана;

УБИ.128: Угроза подмены доверенного пользователя;

УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS;

УБИ.130: Угроза подмены содержимого сетевых ресурсов;

УБИ.131: Угроза подмены субъекта сетевого доступа;

УБИ.132: Угроза получения предварительной информации об объекте защиты;

УБИ.139: Угроза преодоления физической защиты;

УБИ. 140: Угроза приведения системы в состояние «отказ в обслуживании»;

УБИ. 143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.144: Угроза программного сброса пароля BIOS;

УБИ.145: Угроза пропуска проверки целостности программного обеспечения;

УБИ.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.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.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.162: Угроза эксплуатации цифровой подписи программного кода;

УБИ.163: Угроза перехвата исключения/сигнала из привилегированного блока функций;

УБИ.165: Угроза включения в проект не достоверно испытанных компонентов;

УБИ.166: Угроза внедрения системной избыточности;

УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов;

УБИ. 169: Угроза наличия механизмов разработчика;

УБИ. 170: Угроза неправомерного шифрования информации;

УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ.173: Угроза «спама» веб-сервера;

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.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.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.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.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.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 обеспечением 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.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

Обоснование неприменимости угроз к ИВК в связи с отсутствием технологий представлено в таблице 2.

Таблица 2. Обоснование неприменимости угроз к ИВК.

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
1.	Грид-системы	ИВК не является грид-системой	УБИ.001, УБИ.002, УБИ.047, УБИ.081, УБИ.110, УБИ.147
2.	Суперкомпьютеры	В ИВК не применяются суперкомьютеры	УБИ.029, УБИ.082, УБИ.106, УБИ.146, УБИ.161
3.	Беспроводной доступ	В ИВК используются только проводные каналы связи. Беспроводные (wi-fi) каналы отсутствуют	УБИ.011, УБИ.083, УБИ.125, УБИ.126, УБИ.133
4.	Облачные технологии	В ИВК не применяются облачные технологии	УБИ.020, УБИ.021, УБИ.040, УБИ.043, УБИ.054, УБИ.055, УБИ.056, УБИ.064, УБИ.065, УБИ.066, УБИ.070, УБИ.096, УБИ.101, УБИ.134, УБИ.135, УБИ.137, УБИ.138, УБИ.141,

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
			УБИ.142, УБИ.164
5.	Хранилище больших данных	В ИВК не применяются хранилища больших данных	УБИ.038, УБИ.050, УБИ.057, УБИ.060, УБИ.097, УБИ.105, УБИ.136, УБИ.148
6.	Числовое программное управление	В ИВК не применяется числовое программное управление	УБИ.112, УБИ.206, УБИ.207
7.	Веб-сервисы и сторонние прило-жения (браузеры, социальные сети, электронная почта и др.)	В ИВК не используются различные веб-сервисы, браузеры и сторонние приложения, такие как: социальные сервисы, электронная почта.	УБИ.016, УБИ.041, УБИ.042, УИБ.62 УБИ.151, УБИ.159, УБИ.168, УБИ.172, УБИ.173, УБИ.174, УБИ.175, УБИ.201, УБИ.215
8.	Smart-карты типа Java Card	В ИВК не применяются smart-карты	УБИ.216
9.	Мобильные устройства	В ИВК не используются мобильные устройства	УБИ.184, УБИ.194, УБИ.196, УБИ.199, УБИ.200, УБИ.202

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ИВКЭ

При обработке информации на уровне ИВКЭ возможна реализация следующих УБИ:

угрозы информации, обрабатываемой в технических средствах ИВКЭ;

угрозы информации, обрабатываемой в АРМ операторов ИВКЭ;

угрозы утечки видовой информации;

угрозы преднамеренного искажения системного времени в компонентах ИСУЭ.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических

средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИВКЭ.

Угрозы НСД в ИВКЭ связаны с действиями нарушителей, имеющих доступ к ИВКЭ, включая операторов АРМ, реализующих угрозы непосредственно в ИВКЭ. Кроме этого, источниками угроз НСД к информации в ИВКЭ могут быть нарушители с различным потенциалом, а также аппаратные закладки и вредоносные программы.

В ИВКЭ возможны все виды уязвимостей в том числе: уязвимости в микропрограммном, общесистемном, прикладном программном обеспечение, уязвимости, связанные с используемыми протоколами передачи данных, уязвимости, в связи с возможностью наличия аппаратных закладок, уязвимости связанные с недостатками организации ТЗИ от НСД, уязвимости в СЗИ.

В ИВКЭ в соответствии с используемыми технологиями, объектами воздействия, уязвимостями возможны следующие угрозы из Банка данных угроз безопасности информации ФСТЭК России:

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 и/или повторного использования аутентификационной информации;

УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS;

УБИ.010: Угроза выхода процесса за пределы виртуальной машины;

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.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 информационной; (автоматизированной) 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 дентификации/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.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS;

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;

УБИ.048: Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

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. 053: Угроза невозможности управления правами пользователей BIOS;

УБИ.058: Угроза неконтролируемого роста числа виртуальных машин;

УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;

УБИ.061: Угроза некорректного задания структуры данных транзакции;

УБИ.063: Угроза некорректного использования функционала программного и аппаратного обеспечения;

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

УБИ.069[3]: Угроза неправомерных действий в каналах связи;

---

[3] Угроза нейтрализуется с помощью СКЗИ на канале связи между ИВК и ИВКЭ.

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.083[4]: Угроза несанкционированного доступа к системе по беспроводным каналам;

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;

---

[4] Угроза нейтрализуется с помощью СКЗИ на канале связи между ИВК и ИВКЭ.

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.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

УБИ.099: Угроза обнаружения хостов;

УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации;

УБИ.102: Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ.103: Угроза определения типов объектов защиты;

УБИ.104: Угроза определения топологии вычислительной сети;

УБИ.107: Угроза отключения контрольных датчиков;

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.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.127: Угроза подмены действия пользователя путём обмана;

УБИ.128: Угроза подмены доверенного пользователя;

УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS;

УБИ.130: Угроза подмены содержимого сетевых ресурсов;

УБИ.131: Угроза подмены субъекта сетевого доступа;

УБИ.132: Угроза получения предварительной информации об объекте защиты;

УБИ.139: Угроза преодоления физической защиты;

УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»;

УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.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.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.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.162: Угроза эксплуатации цифровой подписи программного кода;

УБИ.163: Угроза перехвата исключения/сигнала из привилегированного блока функций;

УБИ.165: Угроза включения в проект не достоверно испытанных компонентов;

УБИ.166: Угроза внедрения системной избыточности;

УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов;

УБИ. 169: Угроза наличия механизмов разработчика;

УБИ. 170: Угроза неправомерного шифрования информации;

УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ.173: Угроза «спама» веб-сервера;

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.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.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.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.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.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 обеспечением 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.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

Обоснование неприменимости угроз к ИВКЭ в связи с отсутствием технологий представлено в таблице 3.

Таблица 3. Обоснование неприменимости угроз к ИВКЭ.

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
1.	Грид-системы	ИВКЭ не является грид-системой	УБИ.001, УБИ.002, УБИ.047, УБИ.081, УБИ.110, УБИ.147
2.	Суперкомпьютеры	В ИВКЭ не применяются суперкомьютеры	УБИ.029, УБИ.082, УБИ.106, УБИ.146, УБИ.161
3.	Беспроводной доступ	В ИВКЭ используются только проводные каналы связи. Беспроводные (wi-fi) каналы отсутствуют	УБИ.011, УБИ.083, УБИ.125, УБИ.126, УБИ.133
4.	Облачные технологии	В ИВКЭ не применяются облачные технологии	УБИ.020, УБИ.021, УБИ.040, УБИ.043, УБИ.054, УБИ.055, УБИ.056, УБИ.064, УБИ.065, УБИ.066, УБИ.070, УБИ.096, УБИ.101, УБИ.134, УБИ.135, УБИ.137, УБИ.138, УБИ.141, УБИ.142, УБИ.164
5.	Хранилище больших данных	В ИВКЭ не применяются хранилища больших данных	УБИ.038, УБИ.050, УБИ.057, УБИ.060, УБИ.097, УБИ.105, УБИ.136, УБИ.148
6.	Числовое программное управление	В ИВКЭ не применяется числовое программное управление	УБИ.112, УБИ.206, УБИ.207
7.	Веб-сервисы и сторонние прило-жения (браузеры, социальные сети, электронная почта и др.)	В ИВКЭ не используются различные веб-сервисы, браузеры и сторонние приложения, такие как: социальные сервисы, электронная почта.	УБИ.016, УБИ.041, УБИ.042, УИБ.62 УБИ.151, УИБ 173, УБИ.159, УБИ.168, УБИ.172, УБИ.173, УБИ.174, УБИ.175, УБИ.201, УБИ.215
8.	Smart-карты типа Java Card	В ИВКЭ не применяются smart-карты	УБИ.216
9.	Мобильные устройства	В ИВКЭ не используются мобильные устройства	УБИ.184, УБИ.194, УБИ.196, УБИ.199, УБИ.200, УБИ.202
10.	Технология	В ИВКЭ отсутствуют	УБИ.010, УБИ.020,

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
	виртуализации	технологии виртуализации (гипервизоры, виртуальные машины, виртуальные устройства и др.)	УБИ.044, УБИ.046, УБИ.048, УБИ.052, УБИ.058, УБИ.059, УБИ.073, УБИ.075, УБИ.076, УБИ.077, УБИ.078, УБИ.079, УБИ.080, УБИ.084, УБИ.085, УБИ.108, УБИ.119, УБИ.120

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ПУ

При обработке информации на уровне ПУ возможна реализация следующих УБИ:

угрозы информации, обрабатываемой в технических средствах ПУ;

угрозы НСД в ПУ связаны с действиями нарушителей, имеющих доступ к ПУ. Кроме этого, источниками угроз НСД к информации в ПУ могут быть нарушители с различным потенциалом, а также аппаратные закладки и вредоносные программы;

угрозы преднамеренного искажения системного времени в компонентах ИСУЭ.

В ПУ возможны уязвимости в микропрограммном обеспечении, уязвимости, связанные с используемыми протоколами передачи данных, уязвимости, в связи с возможностью наличия аппаратных закладок, уязвимости связанные с недостатками организации ТЗИ от НСД, уязвимости в СЗИ.

В ПУ в соответствии с используемыми технологиями, объектами воздействия, уязвимостями возможны следующие угрозы из Банка данных угроз безопасности информации ФСТЭК России:

УБИ.006: Угроза внедрения кода или данных;

УБИ.007: Угроза воздействия на программы с высокими привилегиями;

УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации;

УБИ.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 информационной; (автоматизированной) системы;

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 дентификации/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.035: Угроза использования слабых криптографических алгоритмов BIOS;

УБИ.036: Угроза исследования механизмов работы программы;

УБИ.037: Угроза исследования приложения через отчёты об ошибках;

УБИ.049: Угроза нарушения целостности данных кеша;

УБИ.061: Угроза некорректного задания структуры данных транзакции;

УБИ.063: Угроза некорректного использования функционала программного и аппаратного обеспечения;

УБИ.069[5]: Угроза неправомерных действий в каналах связи;

---

[5] Указанная угроза может быть нейтрализована без применения СКЗИ

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

УБИ.083[6]: Угроза несанкционированного доступа к системе по беспроводным каналам;

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.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

УБИ.099: Угроза обнаружения хостов;

УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации;

УБИ.102: Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ.103: Угроза определения типов объектов защиты;

УБИ.104: Угроза определения топологии вычислительной сети;

---

[6] Указанная угроза может быть нейтрализована без применения СКЗИ.

УБИ.107: Угроза отключения контрольных датчиков;

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.124: Угроза подделки записей журнала регистрации событий;

УБИ.127: Угроза подмены действия пользователя путём обмана;

УБИ.128: Угроза подмены доверенного пользователя;

УБИ.130: Угроза подмены содержимого сетевых ресурсов;

УБИ.131: Угроза подмены субъекта сетевого доступа;

УБИ.132: Угроза получения предварительной информации об объекте защиты;

УБИ.139: Угроза преодоления физической защиты;

УБИ. 140: Угроза приведения системы в состояние «отказ в обслуживании»;

УБИ. 143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.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.156: Угроза утраты носителей информации;

УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.162: Угроза эксплуатации цифровой подписи программного кода

УБИ.163: Угроза перехвата исключения/сигнала из привилегированного блока функций;

УБИ.165: Угроза включения в проект не достоверно испытанных компонентов;

УБИ.166: Угроза внедрения системной избыточности;

УБИ. 169: Угроза наличия механизмов разработчика;

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.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.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.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.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы;

УБИ.198: Угроза скрытной регистрации вредоносной программой учетных записей администраторов;

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.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.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

Обоснование неприменимости угроз к ПУ в связи с отсутствием технологий представлено в таблице 4.

Таблица 4. Обоснование неприменимости угроз к ПУ в связи с отсутствием технологий.

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
1.	Грид-системы	ПУ не является грид-системой	УБИ.001, УБИ.002, УБИ.047, УБИ.081, УБИ.110, УБИ.147
2.	Суперкомпьютеры	В ПУ не применяются суперкомьютеры	УБИ.029, УБИ.082, УБИ.106, УБИ.146, УБИ.161
3.	Беспроводной доступ	В ПУ не используются беспроводные (wi-fi) каналы	УБИ.011, УБИ.083, УБИ.125, УБИ.126, УБИ.133
4.	Облачные технологии	В ПУ не применяются облачные технологии	УБИ.020, УБИ.021, УБИ.040, УБИ.043, УБИ.054, УБИ.055, УБИ.056, УБИ.064,

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
			УБИ.065, УБИ.066, УБИ.070, УБИ.096, УБИ.101, УБИ.134, УБИ.135, УБИ.137, УБИ.138, УБИ.141, УБИ.142, УБИ.164
5.	Хранилище больших данных	В ПУ не применяются хранилища больших данных	УБИ.038, УБИ.050, УБИ.057, УБИ.060, УБИ.097, УБИ.105, УБИ.136, УБИ.148
6.	Числовое программное управление	В ПУ не применяется числовое программное управление	УБИ.112, УБИ.206, УБИ.207
7.	Веб-сервисы и сторонние прило-жения (браузеры, социальные сети, электронная почта, cookies и др.)	ПУ не используются различные веб-сервисы, браузеры и сторонние приложения, такие как: социальные сервисы, электронная почта.	УБИ.017, УБИ.016, УБИ.041, УБИ.042, УИБ.62 УБИ.151, УИБ 173, УБИ.159, УБИ.168, УБИ.172, УБИ.173, УБИ.174, УБИ.175 УБИ.197, УБИ.201, УБИ.215
8.	Smart-карты типа Java Card	В ПУ не применяются smart-карты	УБИ.216
9.	Мобильные устройства	В ПУ не используются мобильные устройства	УБИ.184, УБИ.194, УБИ.196, УБИ.199, УБИ.200, УБИ.202
10.	Технология виртуализации	В ПУ отсутствуют технологии виртуализации (гипервизоры, виртуальные машины, виртуальные устройства и др.)	УБИ.010, УБИ.020, УБИ.044, УБИ.046, УБИ.048, УБИ.052, УБИ.058, УБИ.059, УБИ.073, УБИ.075, УБИ.076, УБИ.077, УБИ.078, УБИ.079, УБИ.080, УБИ.084, УБИ.085, УБИ.108, УБИ.119, УБИ.120
11.	Наличие BIOS/UEFI	В ПУ отсутствуют технологии BIOS/UEFI	УБИ.004, УБИ.005, УБИ.009, УБИ.013 УБИ.018, УБИ.024, УБИ.032, УБИ.035, УБИ.039, УБИ.045, УБИ.053, УБИ.072,

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
			УИБ.087, УБИ.123, УБИ.129, УБИ.144, УБИ.150, УБИ.154
12.	Наличие ПЭВМ	В при реализации ПУ не применяются ПЭВМ	УБИ.051, УБИ.074, УБИ.167, УБИ.186, УБИ.190, УБИ.203, УБИ.211
13.	Наличие API	В ПУ отсутствуют технологии API	УБИ.068
14.	Наличие машинного носителя информации	В ПУ не применяются внешние носители информации.	УБИ.071, УБИ.158