

**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>

Руководителям сетевых организаций и
гарантирующих поставщиков

11.12.2024 № СЦ-21040/07

На № _____ от _____

О внесении изменений в базовую модель
угроз безопасности информации в
интеллектуальных системах учета
электрической энергии (мощности)

Уважаемые коллеги!

Министерством энергетики Российской Федерации совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю принято решение о внесении изменений в разработанную 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)» базовую модель угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности) (далее – Модель угроз, ИСУ), предусматривающих:

компенсирующие меры, направленные на нейтрализацию угроз УБИ.069 и УБИ.083 в трехуровневой ИСУ с применением ИВКЭ;

использование типовых частных моделей угроз безопасности информационного взаимодействия между компонентами ИСУ;

регламент информирования об оборудовании, получившем положительное заключение ФСБ России об оценке влияния.

В трехуровневой ИСУ при применении прилагаемых к Модели угроз компенсирующих мер угрозы УБИ.069 и УБИ.083 могут быть нейтрализованы без применения средств криптографической защиты информации в приборах учета электрической энергии.

В двухуровневой ИСУ необходимость использования средств криптографической защиты информации в приборах учета электрической энергии будет определена после проведения дополнительных испытаний в соответствии с пунктом 2 раздела III протокола совещания у Заместителя Председателя Правительства Российской Федерации А.В. Новака от 08.12.2022 № АН-П51-131пр.

Приложение: Модель угроз на 294 л.



С.Е. Цивилев

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА
ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	3
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
НОРМАТИВНЫЕ ССЫЛКИ.....	8
ОБЩИЕ ПОЛОЖЕНИЯ.....	9
ОПИСАНИЕ СТРУКТУРНО-ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ИСУЭ	13
ФУНКЦИОНАЛ ИВК	18
ФУНКЦИОНАЛ ИВКЭ.....	20
ФУНКЦИОНАЛ ПУ	22
КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ...	24
МОДЕЛЬ НАРУШИТЕЛЯ ИСУЭ	26
УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ИВК29	
УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ИВКЭ	40
УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ПУ	52
ПРИЛОЖЕНИЯ	60

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 иницилируемый 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 воздействием 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 ХАРАКТЕРИСТИК 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.

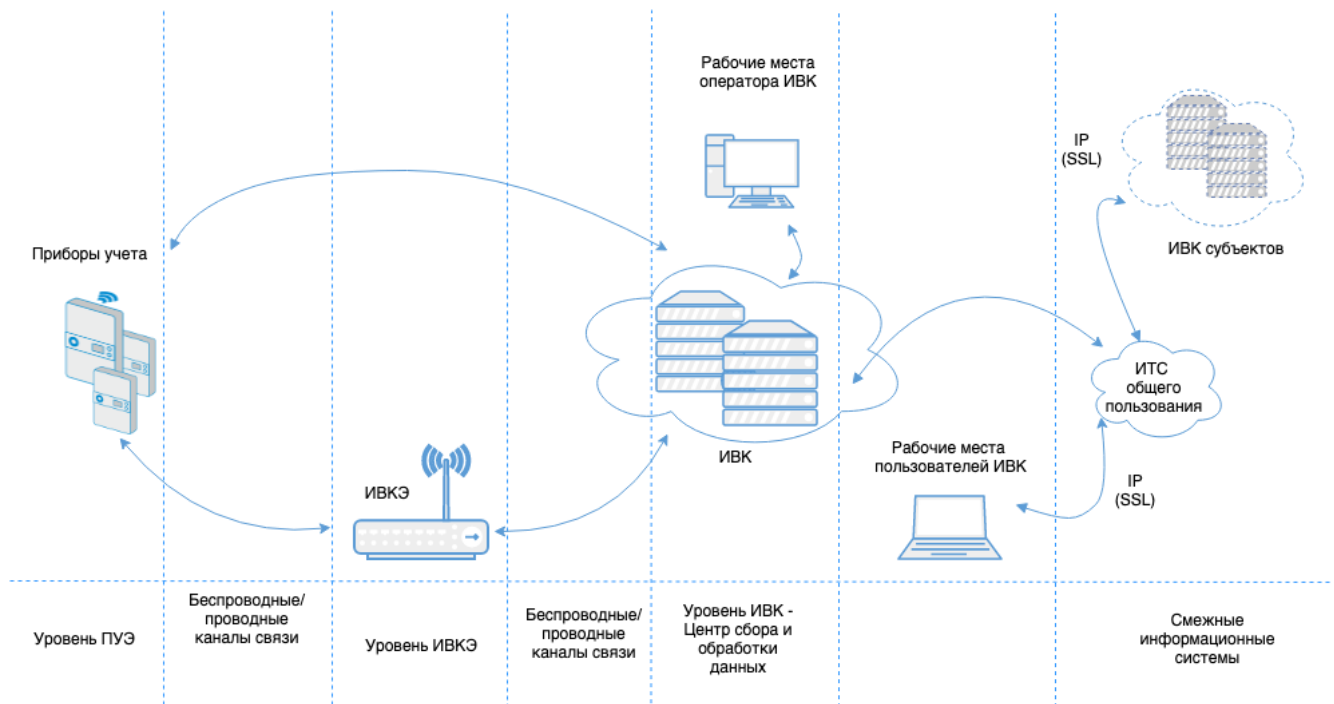


Рисунок 1. Пример общей структурно-коммуникационной схемы ИСУЭ и ПУ

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, лицевого 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 между 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 обеспечении	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	виртуальная машина,	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),

том числе BIOS/UEFI), аппаратное средство, аппаратное устройство	виртуальные 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
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)

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация)реализации угроз безопасности информации	Потенциал нарушителя
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, неосторожные или неквалифицированные действия	Средний (на всех уровнях)
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	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	
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). Мсть 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). Мсть 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. Мсть за ранее совершенные действия.	Средний (на всех уровнях)

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ИБК

При обработке информации на уровне ИБК 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 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 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 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.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.069¹: 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;

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;

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

УБИ.080: Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;

УБИ.083²: 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;

УБИ.095: Угроза несанкционированного управления указателями;

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

УБИ.099: Угроза обнаружения хостов;

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

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 суперкомпьютеры	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, УБИ.142, УБИ.164

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
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 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 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 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.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.069³: Угроза неправомерных действий в каналах связи;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

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

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.083⁴: 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;

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

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 вывода 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 суперкомпьютеры	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 приложения (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, УБИ.62, УБИ.151, УБИ.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 виртуализации	В ИВКЭ отсутствуют технологии	УБИ.010, УБИ.020, УБИ.044, УБИ.046,

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
		виртуализации (гипервизоры, виртуальные машины, виртуальные устройства и др.)	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 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.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^{5,6}: Угроза неправомерных действий в каналах связи;

⁵ В случае использования ИВКЭ (трехуровневая система) и применения компенсирующих мер в соответствии с Приложением №1 к Модели угроз, указанная угроза может быть нейтрализована без применения СКЗИ

⁶ В случае отсутствия ИВКЭ (двухуровневая система), указанная угроза может быть нейтрализована без применения СКЗИ.

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

УБИ.083^{7,8}: 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;

⁷ В случае использования ИВКЭ (трехуровневая система) и применения компенсирующих мер в соответствии с Приложением №1 к Модели угроз, указанная угроза может быть нейтрализована без применения СКЗИ.

⁸ В случае отсутствия ИВКЭ (двухуровневая система), указанная угроза может быть нейтрализована без применения СКЗИ.

- 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.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 вывода 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 суперкомпьютеры	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

№ п/п	Технология	Обоснование неприменимости	Неактуальные угрозы
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, 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

ПРИЛОЖЕНИЕ

К настоящему документу прилагаются:

1. ПРИЛОЖЕНИЕ №1: КОМПЕНСИРУЮЩИЕ МЕРЫ, НАПРАВЛЕННЫЕ НА НЕЙТРАЛИЗАЦИЮ УГРОЗ УБИ.069 И УБИ.083 В ТРЕХУРОВНЕВОЙ ИСУ С ПРИМЕНЕНИЕМ ИВКЭ.
2. ПРИЛОЖЕНИЕ №2: РЕГЛАМЕНТ ИНФОРМИРОВАНИЯ ОБ ОБОРУДОВАНИИ, ПОЛУЧИВШЕМ ПОЛОЖИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ ФСБ РОССИИ ОБ ОЦЕНКЕ ВЛИЯНИЯ.
3. ПРИЛОЖЕНИЕ №3: ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ КОМПОНЕНТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ ВАРИАНТ 1.

4. ПРИЛОЖЕНИЕ №4: ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ КОМПОНЕНТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ ВАРИАНТ 2.
5. ПРИЛОЖЕНИЕ №5: ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ КОМПОНЕНТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ ВАРИАНТ 3.

ПРИЛОЖЕНИЕ № 1

к базовой модели угроз безопасности информации
интеллектуальной системы учета электрической энергии

**КОМПЕНСИРУЮЩИЕ МЕРЫ, НАПРАВЛЕННЫЕ НА
НЕЙТРАЛИЗАЦИЮ УГРОЗ УБИ.069 И УБИ.083 В
ТРЕХУРОВНЕВОЙ ИСУ С ПРИМЕНЕНИЕМ ИВКЭ.**

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ.....	3
ОСНОВНЫЕ ПОЛОЖЕНИЯ	4
ОБЩИЙ АЛГОРИТМ ОГРАНИЧЕНИЯ ПОДАЧИ ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ В ИСУЭ С ПОДТВЕРЖДЕНИЕМ	6

СОКРАЩЕНИЯ

ИВК	–	информационно-вычислительный комплекс
ИВКЭ	–	информационно-вычислительный комплекс электроустановки
ИСУЭ	–	интеллектуальная система учёта электрической энергии (мощности)
ИПУ	–	Индивидуальный прибор учета электрической энергии (мощности)
СКЗИ	–	средства криптографической защиты информации

ОСНОВНЫЕ ПОЛОЖЕНИЯ

В целях исключения значимых негативных последствий по причине несанкционированного воздействия через каналы передачи данных на индивидуальные приборы учета, оборудованные встроенным коммутационным аппаратом (реле), могут быть применены организационные и технические меры, направленные на парирование актуальных угроз информационной безопасности, компенсирующие отсутствие встроенных СКЗИ.

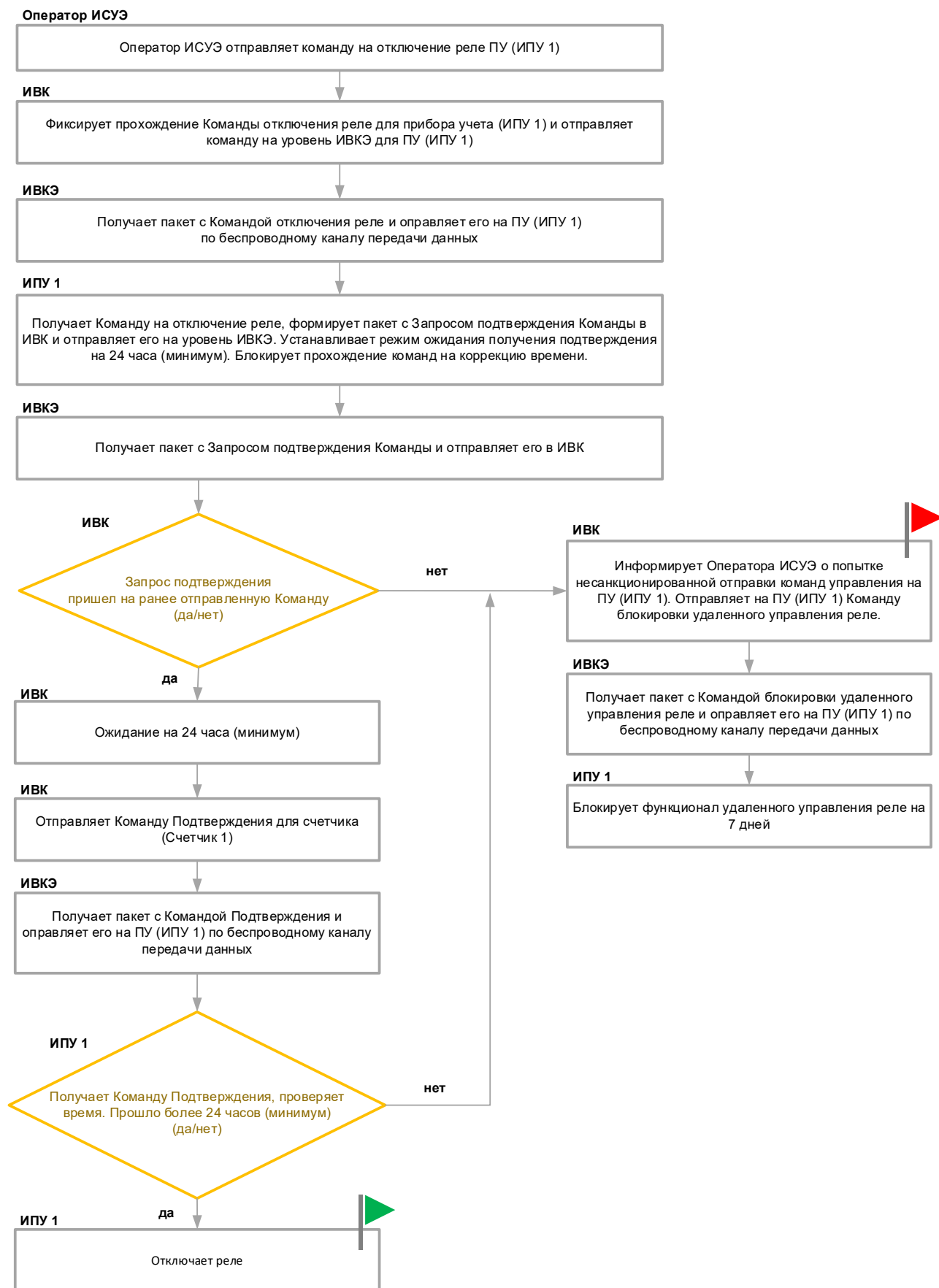
Учитывая специфику функционирования ИСУЭ, ключевым (значимым) негативным последствием, которое может быть вызвано компьютерным инцидентом, является несанкционированное ограничение мощности потребления (отключение электроэнергии) путем передачи команды на отключение реле управления нагрузкой. С учетом последствий, основной категорией показателей значимости для ИСУЭ является «Социальная значимость», а основным показателем — «Прекращение или нарушение функционирования объектов жизнедеятельности населения по показателю «Б» - количество людей, условия жизнедеятельности которых могут быть нарушены (тысячи человек).

Достижение необходимого уровня безопасности может быть обеспечено путем формирования особой логики отправки со стороны ИВК и обработки на ИПУ команд на отключение реле управления нагрузкой с задержкой в 24 часа исполнения, и дополнительным подтверждением со стороны ИВК непосредственно перед исполнением. Данный сценарий выполнения команд на отключение реле обеспечивает безопасность на уровне логики работы системы и будет эффективен при получении злоумышленником кратковременного (до 24 часов) контроля над информационным обменом с прибором учета по каналу передачи данных. Факты получения долговременного контроля канала передачи данных потребуют от злоумышленника необходимости развертывания стационарной

инфраструктуры в непосредственной близости от приборов учета на продолжительный период времени, а также приведут к массовой потере связи ИПУ с ИВК, что, в свою очередь, приведет к реагированию служб эксплуатации энергосбытовой компании и инициированию соответствующего расследования. В случае выявления в ходе расследования признаков целенаправленного несанкционированного воздействия на канал передачи данных, должно быть осуществлено обращение в правоохранительные органы, а на все управляемые ИПУ направлена специальная управляющая команда, блокирующая на 7 суток восприятие прочих управляющих команд (в т.ч. команды на отключение реле), что не позволит злоумышленнику развить атаку, приводящую к значимым последствиям.

Детальная логика реализации компенсирующих мер представлена на схеме «Общий алгоритм ограничения подачи электрической энергии в ИСУЭ с подтверждением»

ОБЩИЙ АЛГОРИТМ ОГРАНИЧЕНИЯ ПОДАЧИ ЭЛЕКТРИЧЕСКОЙ
ЭНЕРГИИ В ИСУЭ С ПОДТВЕРЖДЕНИЕМ



ПРИЛОЖЕНИЕ № 2

к базовой модели угроз безопасности информации
интеллектуальной системы учета электрической энергии

**РЕГЛАМЕНТ ИНФОРМИРОВАНИЯ ОБ ОБОРУДОВАНИИ,
ПОЛУЧИВШЕМ ПОЛОЖИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ ФСБ
РОССИИ ОБ ОЦЕНКЕ ВЛИЯНИЯ.**

Для информирования владельцев ИСУ об оборудовании (ИВКЭ, ИПУ), получившем положительное заключение ФСБ России об оценке влияния оборудования на программное (программно-аппаратное) СКЗИ рекомендован нижеследующий регламент.

1. После получения положительного заключения ФСБ России об оценке влияния оборудования на программное (программно-аппаратное) СКЗИ в течение 20 рабочих дней ФСБ России рекомендовано направить информацию об указанном оборудовании в Минэнерго России. (Состав направляемой информации приведен в следующем разделе.)
2. Минэнерго России в течение 10 рабочих дней после получения информации от ФСБ России рекомендовано опубликовать обновление реестра оборудования, получившего положительное заключение ФСБ России об оценке влияния на программное (программно-аппаратное) СКЗИ, на официальном сайте Минэнерго России в соответствии с приведенным ниже составом информации.

СОСТАВ ИНФОРМАЦИИ ОБ ОБОРУДОВАНИИ, ПОЛУЧИВШЕМ ПОЛОЖИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ ФСБ РОССИИ ОБ ОЦЕНКЕ ВЛИЯНИЯ

Ниже приведена структура информационного сообщения, об оборудовании, получившем положительное заключение ФСБ России об оценке влияния оборудования на программное (программно-аппаратное) СКЗИ, направляемого в Минэнерго России и публикуемом на сайте Минэнерго России.

1. «Наименование оборудования» - полное наименование оборудования, указываемое в паспорте и спецификациях на закупку.
2. «Производитель оборудования» - полное название предприятия, являющегося производителем оборудования.
3. «Встроенное СКЗИ» - полное название СКЗИ, для которого проводилась оценка влияния.
4. «Класс СКЗИ» - класс СКЗИ (КС1, КС2, КС3, КВ, КА).
5. «Производитель СКЗИ» - полное название предприятия, являющегося производителем СКЗИ.
6. «Сертификат соответствия ФСБ России на СКЗИ» - регистрационный номер сертификата ФСБ России на СКЗИ.
7. «Срок действия сертификата соответствия ФСБ России на СКЗИ» - дата истечения срока действия сертификата ФСБ России на СКЗИ.
8. «Заключение ФСБ России об оценке влияния» - номер и дата заключения ФСБ России об оценке влияния оборудования на СКЗИ.
9. «Модель угроз» - Модель угроз, которая использовалась при оценке влияния оборудования на программное (программно-аппаратное) СКЗИ (номер и название приложения из «Базовой модели угроз безопасности информации интеллектуальной системы учета электрической энергии» или регистрационный номер/дата согласования ФСБ России/организация, владелец).

к базовой модели угроз безопасности информации
интеллектуальной системы учета электрической энергии

**ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ
КОМПОНЕНТАМИ**

**ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА
ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ**

ВАРИАНТ 1

Типовая модель угроз программных (программно-аппаратных) средств криптографической защиты информации, применяемых для защиты информационно-вычислительных комплексов электроустановки (устройств сбора и передачи данных) и приборов учета в интеллектуальных системах и средств учёта электрической энергии (мощности)

ОГЛАВЛЕНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ	9
2 НАИМЕНОВАНИЕ СИСТЕМЫ И ЗАКАЗЧИК.....	10
3 ОПИСАНИЕ ИСУЭ	11
3.1 Инфраструктура ИСУЭ	11
3.1.1 Архитектура ИСУЭ	11
3.1.2 Компоненты ИСУЭ.....	12
3.2 Назначение компонент ИСУЭ	14
3.2.1 Назначение ИВК	14
3.2.2 Назначение ИВКЭ.....	15
3.2.3 Назначение ПУ	15
3.3 Функции компонент ИСУЭ	15
3.3.1 Функции ИВК.....	15
3.3.2 Функции ИВКЭ	16
3.3.3 Функции ПУ	17
3.4 Значимая обрабатываемая информация	18
3.5 Организационные, физические и технические меры защиты объектов, на которых располагаются компоненты ИСУЭ	20
3.6 Пользователи ИСУЭ	21
4 ОБОСНОВАНИЕ ИСПОЛЬЗОВАНИЯ И ВЫБОР КЛАССА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	22
4.1 Определение актуальности использования СКЗИ для обеспечения безопасности данных	22
4.1.1 Угрозы, которые могут быть нейтрализованы только с помощью СКЗИ	22
4.1.2 Выводы актуальности использования СКЗИ для обеспечения безопасности данных.....	23

4.2 Этапы разработки, производства, хранения, транспортировки, ввода в эксплуатацию и эксплуатация технических и программных средств, криптосредств и СФК	23
4.3 Объекты защиты и актуальные характеристики безопасности объектов защиты	24
4.4 Классификация и характеристики нарушителей, а также их возможности по реализации атак	26
4.4.1 Определение категорий потенциальных нарушителей	26
4.4.2 Классификация и характеристика потенциальных нарушителей	29
4.5 Обобщенные возможности потенциальных нарушителей	33
5 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ.....	39
6 ОПРЕДЕЛЕНИЕ КЛАССА СКЗИ	41
ПРИЛОЖЕНИЕ А (СПРАВОЧНОЕ) ИСТОЧНИКИ РАЗРАБОТКИ.....	46

СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
ИВК	–	информационно-вычислительный комплекс
ИВКЭ	–	информационно-вычислительный комплекс электроустановки
ИС	–	информационная система
ИСУЭ	–	интеллектуальная система учёта электрической энергии (мощности)
КЗ	–	контролируемая зона
КИИ	–	критическая информационная инфраструктура РФ
ЛЭП	–	линия электропередачи
ПО	–	программное обеспечение
ПУ	–	прибор учета электрической энергии (мощности)
РФ	–	Российская Федерация
СВТ	–	средство вычислительной техники
СКЗИ	–	средства криптографической защиты информации
СОД	–	система обработки данных
СФК	–	среда функционирования криптосредств
УБИ	–	угроза безопасности информации
ФАПСИ	–	Федеральное агентство правительственной связи и информации
ФЗ	–	Федеральный закон
ФСБ	–	Федеральная служба безопасности
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие понятия 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 таким оборудованием и процессами.

автоматизированное рабочее место: Программно-технический комплекс, предназначенный для автоматизированной деятельности определенного вида.

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 N 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.

защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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.

контролируемая зона, КЗ: Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств.

недекларированные возможности: Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

несанкционированный доступ к информации: Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

обработка информации: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

объект доступа: Объект информационной системы, доступ к которому регламентируется правилами разграничения доступа.

оператор: Юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

пароль: Условный набор знаков, служащий для подтверждения полномочий субъекта, который является его (субъекта) секретом.

персональные данные: Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

правила разграничения доступа: Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

ресурс системы: Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

среда функционирования критпосредства, СФК: Совокупность компонентов аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ.

средства вычислительной техники: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

средство криптографической защиты информации, СКЗИ: Программное или программно-аппаратное средство, реализующее алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи.

субъект доступа: Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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, УБИ: Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.

учетная запись пользователя: Набор данных, однозначно идентифицирующих пользователя в системе, совокупность прав и привилегий доступа к объектам и набор квот системных ресурсов.

Уязвимость: Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ предназначен для определения необходимого уровня криптографической защиты информации, обрабатываемой в интеллектуальной системе учета электрической энергии (мощности) (ИСУЭ) с трехуровневой структурно-коммуникационной схемой.

В случае если ИСУЭ имеет сегменты с разной структурно-коммуникационной схемой допустимо использовать настоящий документ для определения необходимого уровня криптографической защиты информации, обрабатываемой в сегменте ИСУЭ с трехуровневой структурно-коммуникационной схемой.

Документ разработан с учётом требований документа [6], разработанного Минэнерго России совместно с Федеральной службой безопасности (ФСБ) Российской Федерации (РФ) и ФСТЭК России, и является неотъемлемым её приложением.

В типовой модели угроз безопасности к объектам защиты отнесены данные, обмен которыми осуществляется между информационно-вычислительным комплексом (ИВК), информационно-вычислительным комплексом электроустановки (ИВКЭ) и приборами учета электрической энергии (мощности) (ПУ) в соответствии с требованиями документа [5].

Разработка данного документа выполнена в соответствии с требованиями законодательства РФ и ведомственных нормативных документов в области защиты информации.

Данная Типовая модель угроз безопасности информационного взаимодействия между ИВК, ИВКЭ и ПУ ИСУЭ разработана с учетом требований нормативных документов, указанных в приложении А.

Настоящая модель подлежит уточнению в случае изменения технологии обработки информации или изменения категории информации, а также в случае изменения требований законодательства РФ в области защиты информации.

2 НАИМЕНОВАНИЕ СИСТЕМЫ И ЗАКАЗЧИК

Полное наименование Системы: Интеллектуальная система учета электрической энергии (мощности).

Краткое наименование системы: ИСУЭ.

Заказчик Системы: гарантирующие поставщики и сетевые организации.

3 ОПИСАНИЕ ИСУЭ

3.1 ИНФРАСТРУКТУРА ИСУЭ

3.1.1 Архитектура ИСУЭ

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

- ИВК;
- ИВКЭ;
- приборы учета электрической энергии.

Типовая структурная схема ИСУЭ представлена на рисунке 1.

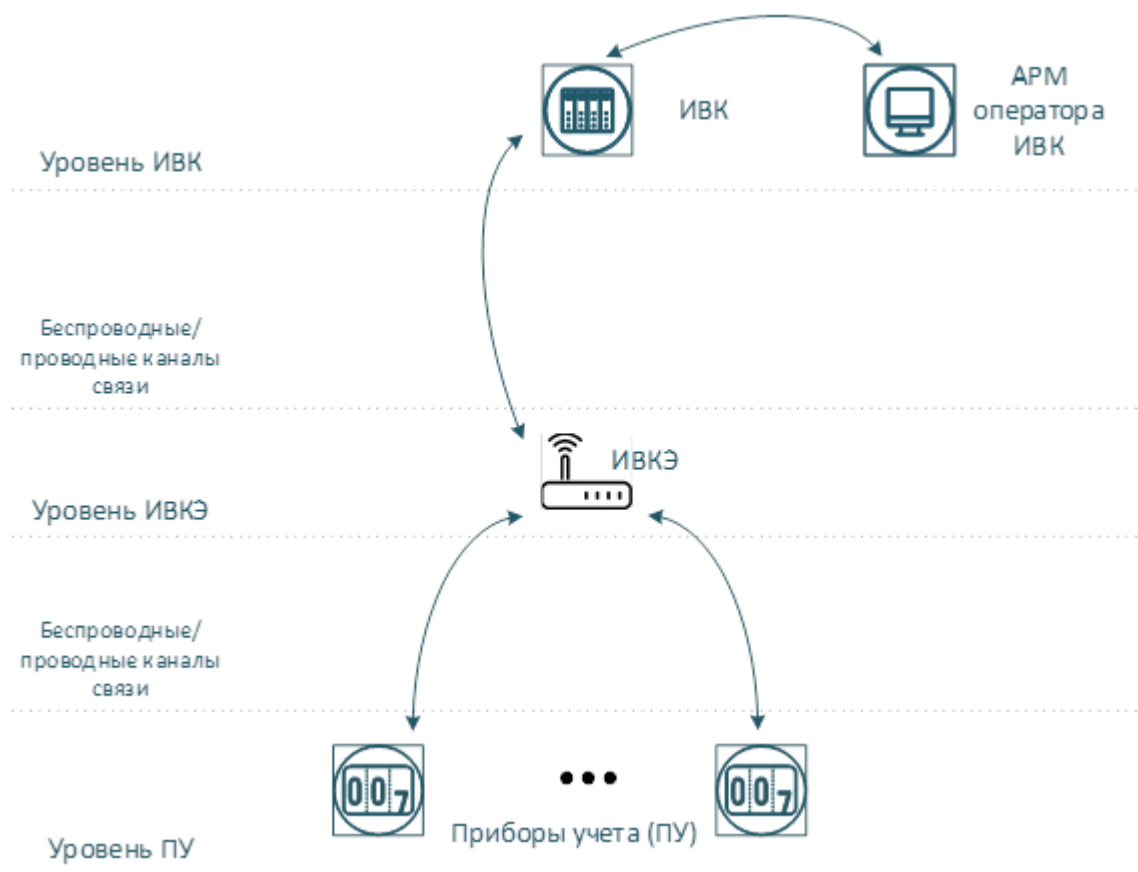


Рисунок 1 – Типовая структурная схема ИСУЭ

3.1.2 Компоненты ИСУЭ

ИВК представляет собой систему, осуществляющую сбор и хранение информации с ПУ, для ее предоставления в личные кабинеты пользователей, имеющих возможность дистанционного подключения, и смежные системы, формирования отчетностей и отображения графиков потребления энергообъектов в целом.

В системе обработки данных (СОД) ИВК обрабатывается целевая информация, персональные данные и иная информация, подлежащая защите в соответствии с требованиями законодательства Российской Федерации в области защиты информации, а также в соответствии с Правилами предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности), утвержденными постановлением Правительства Российской Федерации от 19.06.2020 № 890.

СОД ИВК функционирует внутри контролируемой зоны уровня ИВК.

В соответствии с ГОСТ Р 56115-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования» (пункт 3.1.2) контролируемая зона (КЗ) – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств. КЗ включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Программные и технические элементы СОД ИВК могут быть территориально распределены по различным центрам сбора и обработки данных (далее – сегменты ИВК), при этом передача информации между сегментами ИВК осуществляется по каналам связи, выходящим за пределы контролируемой зоны.

ИВКЭ находится на среднем уровне ИСУЭ. СОД ИВКЭ представляет собой совокупность программных и технических средств для решения задач сбора, хранения, передачи в ИВК данных учета электрической энергии и сопутствующей информации, удаленного управления ПУ и их нагрузкой. Оборудование ИВКЭ располагается вне пределов КЗ и может устанавливаться как внутри монтажного шкафа, так и на монтажных направляющих или рейках на чердаках, в подвалах зданий и опорах. Неконтролируемое пребывание посторонних лиц в помещениях, где расположены технические средства ИВКЭ (включая средства защиты информации при их использовании), не исключается.

ПУ являются средством измерения параметров электрической энергии. ПУ располагаются вне пределов КЗ. ПУ обладает защитой от несанкционированного доступа – датчик несанкционированного вскрытия клеммной крышки, датчик несанкционированного вскрытия корпуса (для разборных корпусов) и защита от воздействия постоянным и переменным магнитным полем. ПУ в рамках городской застройки устанавливаются в электрических щитах квартир или подъездов многоквартирных домов. Для частных домов, кооперативов и дачных участков ПУ устанавливаются в специальных шкафах наружной установки, оснащенных защитой от взлома (замок), на опорах ЛЭП. ПУ имеют прямое взаимодействие с оборудованием ИВКЭ, к которому подключены. Также следует отметить, что неконтролируемое пребывание посторонних лиц в местах размещения ПУ не исключается.

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

ИВК могут взаимодействовать с различными смежными системами.

Порядок взаимодействия и подключения смежных систем к ИВК определяется утвержденным регламентом.

Информационное взаимодействие компонентов и устройств ИСУЭ обеспечивается между:

- СОД ИВК и СОД ИВКЭ – по беспроводным и проводным каналам связи;
- между сегментами ИВК – по проводным каналам связи;
- СОД ИВКЭ и ПУ – по беспроводным, проводным каналам связи и линиям электропередачи.

Технологическое обслуживание (настройка) технических средств СОД ИВКЭ и ПУ обеспечивается специалистами службы эксплуатации по каналам связи или локальным подключением к интерфейсу связи технического средства ИВКЭ или ПУ.

Оборудование, входящее в состав СОД ИВКЭ, может обеспечивать логическое соединение между СОД ИВК и ПУ за счет инкапсулирования протоколов обмена данными СОД ИВК и ПУ для организации прямого соединения между ними.

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

3.2 НАЗНАЧЕНИЕ КОМПОНЕНТ ИСУЭ

3.2.1 Назначение ИВК

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;
- управления ПУ, присоединенными к ИВК через ИВКЭ;
- изменения конфигурационных параметров ИВКЭ и ПУ, а также для обновления программного обеспечения (ПО).

3.2.2 Назначение ИВКЭ

ИВКЭ предназначен для:

- дистанционного считывания, накопления, обработки, хранения и отображения результатов измерений, количества и иных параметров электрической энергии, журналов событий и данных о настройке ПУ по протоколам обмена данными;
- управления ПУ, присоединенными к ИВКЭ;
- изменения конфигурационных параметров ПУ, а также для обновления ПО.

3.2.3 Назначение ПУ

ПУ предназначен для:

- сбора и обработки показаний и результатов измерений ПУ;
- передачи в ИВКЭ событий ПУ;
- приема из ИВКЭ параметров конфигурационных настроек;
- передачи в ИВКЭ информации о несанкционированном вскрытии.

3.3 ФУНКЦИИ КОМПОНЕНТ ИСУЭ

3.3.1 Функции ИВК

Основными функциями ИВК являются:

- 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 РФ;

– обработка событий и оповещение потребителя 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.

Дополнительно ИВК должен обеспечивать выполнение функций управления параметрами конфигурационной настройки ИВКЭ и ПУ, в том числе обновление их программного обеспечения.

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

3.3.2 Функции ИВКЭ

Основными функциями ИВКЭ являются:

– 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 РФ;

- 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 оборудования ИВКЭ и подключаемых ПУ.

3.3.3 Функции ПУ

Основными функциями ПУ являются:

- 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».

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 (полукошвенного подключения);

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

Встроенное реле управления нагрузкой имеется только у однофазных и трехфазных ПУ 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 ПУ, 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).

3.4 ЗНАЧИМАЯ ОБРАБАТЫВАЕМАЯ ИНФОРМАЦИЯ

Значимой информацией, обрабатываемой в ИСУЭ, является:

а) для СОД ИВК:

- команды управляющих воздействий (управление коммутацией реле нагрузки);
- события безопасности ПУ и ИВКЭ (контроль доступа, воздействия магнитным полем на элементы ПУ, неработоспособность ПУ вследствие аппаратного или программного сбоя, его отключения после повторного включения, перезагрузки);

- результаты измерений количества и иных параметров электрической энергии (мощности) ПУ;
- параметры профилей нагрузки, времени, профилей телеизмерений и телесигнализации, обслуживаемых ПУ;
- параметры идентификации (аутентификации) ПУ (уникальных логических имен);
- персональные данные (данные пользователей и их лицевые счета, а также учетные данные обслуживающего персонала)¹.

б) для СОД ИВКЭ:

- результаты измерений, количества и иных параметров электрической энергии (мощности) ПУ;
- параметры профилей нагрузки, 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) для ПУ:

- результаты измерений, количества и иных параметров электрической энергии (мощности);
- параметры профиля загрузки, времени;
- управляющая (командная) информация;
- параметры идентификации (аутентификации) (уникальное логическое имя);

¹ В соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» персональные данные подлежат обязательной защите.

- события, связанные с током, напряжением, включение/выключением ПУ, программирования параметров ПУ, внешним воздействием, с коммуникационными событиями, с контролем доступа);
- параметры сетевой настройки устройств связи.

3.5 ОРГАНИЗАЦИОННЫЕ, ФИЗИЧЕСКИЕ И ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ОБЪЕКТОВ, НА КОТОРЫХ РАСПОЛАГАЮТСЯ КОМПОНЕНТЫ ИСУЭ

Помещения, в которых расположены компоненты ИВК (технические средства СОД, коммутационное оборудование, автоматизированные рабочие места (АРМ) пользователей, средства криптографической защиты информации (СКЗИ) и пр.), обеспечиваются комплексом технических средств охраны, включая видеонаблюдение, охранную и пожарную сигнализации, систему контроля и управления доступом.

В ИВК на основании организационно-распорядительных документов владельца ИСУЭ также выполнены следующие организационные мероприятия:

- организована контролируемая зона;
- организован пропускной режим.

Технические средства ИВКЭ устанавливаются вне контролируемой зоны. Организация контролируемой зоны на уровне ИВКЭ не представляется возможной. Могут быть реализованы лишь ограничения возможностей нарушителя по организации атак. Для ограничения возможностей нарушителя по организации атак монтажные шкафы, в которых размещаются технические средства ИВКЭ, могут быть оборудованы датчиками вскрытия.

В случае срабатывания датчиков:

- блокируется штатная работа технических средств ИВКЭ;
- стирается настроечная и ключевая информация (в случае использования СКЗИ);
- обеспечивается передача сообщения в ИВК о несанкционированном доступе.

ПУ оборудованы датчиками фиксации несанкционированного доступа.

В случае срабатывания датчиков:

- блокируется штатная работа ПУ;
- обеспечивается передача сообщения в ИВКЭ о несанкционированном доступе.

3.6 ПОЛЬЗОВАТЕЛИ ИСУЭ

Минимальный перечень пользовательских ролей, необходимых для реализации разграничения прав пользователей в ИСУЭ, приведен в таблице 1.

Т а б л и ц а 1 – Перечень пользовательских ролей ИСУЭ

Пользовательская роль	Описание
Администратор СОД	Роль, позволяющая: – добавлять/удалять пользователей СОД; – управление правами доступа пользователей к СОД
Администратор технических средств	Роль, позволяющая: – добавлять/удалять операторов службы эксплуатации; – управлять правами операторов службы эксплуатации
Оператор службы эксплуатации	Настраиваемая роль в зависимости от бизнес-процессов. Роль, позволяющая: – управлять оборудованием СОД; – валидировать реестры заявок из ИВК на управление нагрузкой; – просмотр журналов системы СОД
Администратор средств защиты информации	Роль, позволяющая: – добавлять/удалять пользователей СКЗИ; – функционирующих в ИСУЭ; – управление правами доступа пользователей к СКЗИ, функционирующих в ИСУЭ

П р и м е ч а н и е – Перечень пользовательских ролей ИСУЭ может быть изменен в зависимости от организационно-штатной структуры ИСУЭ конкретной организации. Роли Администратора СОД, Администратора технических средств и Администратора средств защиты информации являются самостоятельными ролями и не могут быть совмещены для одного физического лица.

4 ОБОСНОВАНИЕ ИСПОЛЬЗОВАНИЯ И ВЫБОР КЛАССА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ ИСПОЛЬЗОВАНИЯ СКЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

4.1.1 Угрозы, которые могут быть нейтрализованы только с помощью СКЗИ

В соответствии с документом [6], разработанным Министерством энергетики РФ совместно с ФСБ РФ, ФСТЭК и Министерством цифрового развития, связи и массовых коммуникаций РФ, определены угрозы, которые могут быть нейтрализованы только с помощью СКЗИ:

УБИ.069² – Угроза неправомерных действий в каналах связи: при передаче данных (информации) по каналам связи (включая каналы связи между сегментами ИВК в случае распределенной архитектуры ИВК), не защищенным от перехвата нарушителем, передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

Перечень передаваемой информации приведен в подразделе 3.4;

УБИ.083 – Угроза несанкционированного доступа к системе по беспроводным каналам: при передаче данных (информации) по беспроводным каналам связи, не защищенным от перехвата нарушителем, передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

² В соответствии с классификацией Банка данных угроз безопасности информации ФСТЭК России.

4.1.2 Выводы актуальности использования СКЗИ для обеспечения безопасности данных

Для обеспечения конфиденциальности и целостности данных и информации, передаваемой между СОД ИВКЭ и СОД ИВК по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию, необходимо применение СКЗИ.

4.2 ЭТАПЫ РАЗРАБОТКИ, ПРОИЗВОДСТВА, ХРАНЕНИЯ, ТРАНСПОРТИРОВКИ, ВВОДА В ЭКСПЛУАТАЦИЮ И ЭКСПЛУАТАЦИЯ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ, КРИПТОСРЕДСТВ И СФК

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств, криптосредств и среды функционирования криптосредств (СФК) обработка данных не производится. Поэтому объектами атак могут быть только сами эти средства и документация на них.

В связи с изложенным, на указанных этапах возможны следующие атаки:

- внесение негативных функциональных возможностей в технические и программные средства, криптосредства и СФК, в том числе с использованием вредоносных программ (компьютерные вирусы, «тройанские кони» и т. д.);
- внесение несанкционированных изменений в документацию на технические и программные средства, криптосредство и СФК.

Следует отметить, что указанные атаки:

- на этапах разработки, производства и технических и программных средств, криптосредств и СФК могут проводиться только вне зоны ответственности Заказчика;
- на этапе транспортировки технических средств, криптосредств и СФК могут проводиться как в зоне, так и вне зоны ответственности Заказчика;

– на этапе хранения технических и программных средств, криптосредств и СФК могут проводиться как в зоне, так и вне зоны ответственности Заказчика;

– на этапе ввода в эксплуатацию технических и программных средств, криптосредств и СФК могут проводиться как в зоне, так и вне зоны ответственности Заказчика.

В связи с этим Заказчику необходимо провести:

– проверку соответствия технических и программных средств, криптосредств и СФК и документации на эти средства, поступающих в зону ответственности Заказчика, эталонным образцам;

– проверку целостности технических и программных средств, криптосредств, СФК и документации на эти средства в процессе хранения и ввода в эксплуатацию этих средств³.

4.3 ОБЪЕКТЫ ЗАЩИТЫ И АКТУАЛЬНЫЕ ХАРАКТЕРИСТИКИ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЗАЩИТЫ

Согласно [6] к объектам защиты должны быть отнесены данные, обмен которыми осуществляется между компонентами ИСУЭ по каналам связи, а также СКЗИ и СФК.

Сводный перечень объектов защиты ИСУЭ и их характеристик безопасности, которые должны обеспечиваться, представлен в таблице 2.

В таблице приняты следующие обозначения:

«+»: характеристики безопасности, которые должны быть обеспечены;

«-»: отсутствует необходимость обеспечения характеристики безопасности.

³ С использованием как механизмов контроля, описанных в документации, например, на криптосредство, так и с использованием организационных и организационно-технических мер, разработанных оператором с учетом требований соответствующих нормативных и методических документов

Т а б л и ц а 2 – Сводный перечень объектов защиты ИСУЭ

Объект защиты		Характеристики безопасности	
		К	Ц
ИВК			
Данные и информация управляющих воздействий, передаваемые по каналам связи между СОД ИВК и СОД ИВКЭ		+	+
Данные и информация управляющих воздействий, передаваемые по каналам связи между сегментами СОД ИВК		+	+
Сведения об ИВК	конфигурационные настройки, системные файлы, исполняемые файлы системного ПО	–	+
	конфигурационные настройки, системные файлы, исполняемые файлы прикладного ПО	–	+
	конфигурационные настройки коммуникационного оборудования	–	+
	учетные данные пользователей	+	+
	учетные данные администраторов, атрибуты доступа к интерфейсам управления	+	+
Средства криптографической защиты и среда функционирования криптосредства		+	+
ИВКЭ			
Данные, передаваемые по каналам связи между СОД ИВКЭ и СОД ИВК		+	+
Сведения об ИВКЭ	конфигурационные настройки, системные файлы, исполняемые файлы системного ПО	–	+
	конфигурационные настройки, системные файлы, исполняемые файлы прикладного ПО	–	+
	конфигурационные настройки коммуникационного оборудования	–	+
Средства криптографической защиты и среда функционирования криптосредства		+	+
Документация и иное			
Ключевая, парольная и аутентифицирующая информация СКЗИ		+	+
Документация на СКЗИ		–	+
Проектная документация ИСУЭ		+	+
Записи журналов регистрации СКЗИ		+	+

4.4 КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКИ НАРУШИТЕЛЕЙ, А ТАКЖЕ ИХ ВОЗМОЖНОСТИ ПО РЕАЛИЗАЦИИ АТАК

4.4.1 Определение категорий потенциальных нарушителей

Перечень предполагаемых нарушителей безопасности информации и их краткое описание приведены в таблице 3.

Т а б л и ц а 3 – Описание потенциальных нарушителей, в зависимости от прав доступа к ИСУЭ

Индекс категории		Потенциальные нарушители	Описание
КН1.1		Обслуживающий персонал и прочие лица	<p>К данной категории относятся лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие санкционированного доступа к техническим средствам и информационным ресурсам СОД ИВК:</p> <ul style="list-style-type: none"> – уборщики помещений (в том числе серверных комнат), в которых расположены технические средства СОД ИВК; – лица, ответственные за функционирование пожарно-охранной системы помещений (в том числе серверных комнат), в которых расположены технические средства СОД ИВК; – лица, ответственные за обеспечение электроснабжения помещений (в том числе серверных комнат), в которых расположены технические средства СОД ИВК; – прочие лица, имеющие санкционированный доступ в помещения (в том числе серверные комнаты), в которых расположены технические средства СОД ИВК
КН1.2	КН1.2.1	Пользователи, работающие в пределах контролируемой зоны	К данной категории относятся зарегистрированные пользователи СОД ИВК, осуществляющие доступ из пределов контролируемой зоны, указанные лица имеют санкционированный доступ к техническим средствам

Индекс категории		Потенциальные нарушители	Описание
	КН1.2.2	Пользователи системы, работающие в контролируемых зонах сегментов ИВК	К данной категории относятся зарегистрированные пользователи СОД ИВК – сотрудники, осуществляющие удаленный доступ по защищенным каналам связи из сегментов ИВК. Эти пользователи не имеют физического доступа к СОД ИВК и не имеют доступа к инфраструктуре управления
КН1.3	КН1.3.1	Администраторы ИСУЭ	К данной категории относятся зарегистрированные пользователи СОД ИВК и СОД ИВКЭ с полномочиями администратора СОД и администратора средств защиты информации. Данная категория потенциальных нарушителей имеет полный доступ к средствам защиты информации и протоколирования, а также к части технических средств СОД ИВК
	КН1.3.2	Лица, производящие настройку и установку оборудования, взаимодействующего с СКЗИ	Лица – сотрудники подрядчика, монтажники, которые осуществляют санкционированный доступ к оборудованию СОД ИВК и СОД ИВКЭ, взаимодействующему с СКЗИ. Данные лица не имеют доступа к самому СКЗИ. Лица не заинтересованы в нарушении работоспособности СКЗИ
КН.1.4		Администраторы технических средств	К данной категории относятся зарегистрированные пользователи СОД ИВК и СОД ИВКЭ с полномочиями администратора технических средств. Данная категория потенциальных нарушителей имеет доступ ко всем техническим средствам обработки информации и данным СОД ИВК/ИВКЭ, обладает правами конфигурирования и административной настройки технических средств
КН.1.5		Лица, осуществляющие сопровождение программного обеспечения	К данной категории относятся программисты-разработчики прикладного программного обеспечения, а также лица, обеспечивающие его сопровождение в пределах контролируемой зоны СОД ИВК/ИВКЭ. Данная категория потенциальных нарушителей имеет санкционированный доступ к информационным ресурсам и техническим средствам
КН.1.6		Лица, обеспечивающие поставку, установку, настройку,	К данной категории относятся лица, обеспечивающие поставку, установку, настройку, сопровождение и ремонт технических средств.

Индекс категории	Потенциальные нарушители	Описание
	сопровождение и ремонт, обслуживание технических средств	Данная категория потенциальных нарушителей имеет доступ к техническим средствам СОД ИВК/ИВКЭ, не имеет санкционированного доступа к информационным ресурсам СОД ИВК. Ремонт оборудования на месте не производится, осуществляется замена на запасное оборудование
КН2.1	Физические лица, не имеющие санкционированного доступа к СОД ИВК/ИВКЭ	К данной категории нарушителей относятся посторонние лица, пытающиеся получить доступ к информации в инициативном порядке, в том числе бывшие или уволенные работники (обида, месть), конкурирующие организации (с целью получения конкурентных преимуществ или нанесения ущерба)

Администраторы СОД, администраторы технических средств и администраторы средств защиты информации относятся к привилегированным пользователям. В отношении указанных работников, обладающих административными полномочиями, проводятся мероприятия по подбору и мотивации персонала, мероприятия, направленные на повышение их ответственности и лояльности.

Лица, производящие настройку и установку оборудования, взаимодействующего с СКЗИ, не имеют доступа к обрабатываемой информации и к самому СКЗИ.

С учётом вышеизложенного, лица категории КН1.3 – КН1.4 не рассматриваются в качестве потенциальных нарушителей информационной безопасности.

Категории лиц, рассматриваемых в качестве нарушителей, приведены в таблицах 4 и 5.

Т а б л и ц а 4 – Перечень потенциальных нарушителей безопасности СОД ИВК

Потенциальный нарушитель		Индекс категории	
Внутренний нарушитель	Обслуживающий персонал, лица имеющие разовый пропуск (посетители)	KN1	KN1.1
	Зарегистрированные пользователи, имеющие санкционированный доступ к СОД ИВК		KN1.2
	Лица, осуществляющие сопровождение программного обеспечения		KN1.5
	Лица, обеспечивающие поставку, установку, настройку, сопровождение и ремонт, обслуживание технических средств		KN1.6
Внешний нарушитель	Физические лица, не имеющие санкционированного доступа к СОД ИВК	KN2	KN2.1

Т а б л и ц а 5 – Перечень потенциальных нарушителей безопасности для СОД ИВКЭ

Потенциальный нарушитель		Индекс категории	
Внутренний нарушитель	Обслуживающий персонал	KN1	KN1.1
	Лица, осуществляющие сопровождение программного обеспечения		KN1.5
	Лица, обеспечивающие поставку, установку, настройку, сопровождение и ремонт, обслуживание технических средств		KN1.6
Внешний нарушитель	Физические лица, не имеющие санкционированного доступа оборудованию СОД ИВКЭ	KN2	KN2.1

4.4.2 Классификация и характеристика потенциальных нарушителей

Возможности нарушителей определяются с учетом результатов анализа прав доступа субъектов к информации и к компонентам СОД ИВК и СОД ИВКЭ.

Анализ прав доступа к компонентам СОД ИВК и СОД ИВКЭ приведен в таблице 6. В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ

к компонентам СОД ИВК или СОД ИВКЭ и (или) содержащейся в ней информации или не иметь такого доступа.

Т а б л и ц а 6

Объект защиты		Возможность доступа нарушителей к объектам защиты				
		КН1.1	КН1.2	КН1.5	КН1.6	КН2.1
СОД ИВК						
Данные и информация управляющих воздействий, передаваемая по каналам связи между СОД ИВК и СОД ИВКЭ		Возможен доступ	Возможен доступ	Возможен доступ	Возможен доступ	Возможен доступ
Данные и информация управляющих воздействий, передаваемая по каналам связи между сегментами СОД ИВК		Возможен доступ	Возможен доступ	Возможен доступ	Возможен доступ	Возможен доступ
Сведения об ИВК	конфигурационные настройки, системные файлы, исполняемые файлы системного и прикладного ПО	Отсутствует	Возможен доступ	Возможен доступ	Отсутствует	Отсутствует
	конфигурационные настройки коммуникационного оборудования	Отсутствует	Возможен доступ	Возможен доступ	Возможен доступ	Отсутствует
	учетные данные пользователей	Отсутствует	Возможен доступ	Возможен доступ	Возможен доступ	Отсутствует
	учетные данные администраторов, атрибуты доступа к интерфейсам управления	Отсутствует	Возможен доступ	Отсутствует	Отсутствует	Отсутствует
Средства криптографической защиты и среда функционирования криптосредства		Отсутствует	Возможен доступ	Отсутствует (доступ в помещения осуществляется только в присутствии ответственного администратора)	Отсутствует (доступ в помещения осуществляется только в присутствии ответственного администратора)	Отсутствует

Объект защиты		Возможность доступа нарушителей к объектам защиты				
		КН1.1	КН1.2	КН1.5	КН1.6	КН2.1
ИВКЭ						
Информация, передаваемая по каналам связи между СОД ИВК и СОД ИВКЭ		Возможен доступ	—	Возможен доступ	Возможен доступ	Возможен доступ
Сведения об ИВКЭ	конфигурационные настройки, системные файлы, исполняемые файлы системного ПО	Отсутствует	—	Возможен доступ	Возможен доступ	Возможен доступ
	конфигурационные настройки, системные файлы, исполняемые файлы прикладного ПО	Отсутствует	—	Возможен доступ	Возможен доступ	Возможен доступ
	конфигурационные настройки коммуникационного оборудования	Отсутствует	—	Возможен доступ	Возможен доступ	Возможен доступ
Средства криптографической защиты и среда функционирования криптосредства		Отсутствует	—	Возможен доступ	Возможен доступ	Возможен доступ
Документация и иное						
Ключевая, парольная и аутентифицирующая информация СКЗИ		Отсутствует	Возможен с используемого АРМ	Отсутствует	Отсутствует	Отсутствует
Документация на СКЗИ		Возможен доступ (к имеющейся в свободном доступе)	Возможен доступ (к имеющейся в свободном доступе)	Возможен доступ (к имеющейся в свободном доступе)	Возможен доступ (к имеющейся в свободном доступе)	Возможен доступ (к имеющейся в свободном доступе)
Записи журналов регистрации СКЗИ		Отсутствует	Отсутствует	Отсутствует	Отсутствует	Отсутствует
Проектная документация ИСУЭ		Отсутствует	Отсутствует	Есть в части выполнения своих целевых функций	Есть в части выполнения своих целевых функций	Отсутствует

4.5 ОБОБЩЕННЫЕ ВОЗМОЖНОСТИ ПОТЕНЦИАЛЬНЫХ НАРУШИТЕЛЕЙ

Обобщённые возможности нарушителя формируются на основании оценки наличия (отсутствия) возможностей у каждой категории нарушителя, Обоснование возможностей нарушителя актуальными или неактуальными приведено в таблице 7.

Уточненные возможности нарушителей приведены в таблице 8.

Т а б л и ц а 7 – Обобщенные возможности нарушителей

Номер	Обобщенные возможности нарушителей	СОД ИВК Да/Нет	СОД ИВКЭ Да/Нет	Примечание
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны	Да	Да	См. таблицу 8
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, в том числе к средствам, на которых реализованы СКЗИ и среда их функционирования	Да	Да	См. таблицу 8
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, в том числе к средствам, на которых реализованы СКЗИ и среда их функционирования	Да	Да	См. таблицу 8
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет	Нет	См. таблицу 8

Номер	Обобщенные возможности нарушителей	СОД ИВК Да/Нет	СОД ИВКЭ Да/Нет	Примечание
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет	Нет	См. таблицу 8
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет	Нет	См. таблицу 8

Т а б л и ц а 8 – Уточненные возможности нарушителей

Номер	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак		Обоснование отсутствия
		Для СОД ИВК	Для СОД ИВКЭ	
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования			
1.1	проведение атаки при нахождении в пределах контролируемой зоны	Актуально	Актуально	
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФК; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФК	Актуально	Актуально	
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФК	Актуально	Актуально	

Номер	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак		Обоснование отсутствия
		Для СОД ИВК	Для СОД ИВКЭ	
1.4	использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	Актуально	
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования			
2.1	физический доступ к средствам вычислительной техники (далее - СВТ), на которых реализованы СКЗИ и СФК	Актуально	Актуально	
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФК, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	Актуально	
3	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)			
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФК, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Неактуально	Неактуально	В части СОД ИВК: – проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с пропускным режимом; – помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; – не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности; – проводятся работы по подбору персонала;

Номер	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак		Обоснование отсутствия
		Для СОД ИВК	Для СОД ИВКЭ	
				<p>– доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с контрольно- пропускным режимом;</p> <p>– помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода;</p> <p>– представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;</p> <p>– осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;</p> <p>– осуществляется регистрация и учет действий пользователей;</p> <p>В части СОД ИВКЭ:</p> <p>– устройства обеспечиваются датчиками вскрытия на заводе-изготовителе. В случае срабатывания удаляется ключевая информация и обмен информацией прекращается;</p> <p>– доступ к операционной системе и прикладному ПО технических средств приема-передачи данных обеспечивается с использованием штатных средств защиты от несанкционированного доступа, встроенных во внутреннюю микропрограмму;</p> <p>– устройства обеспечивают передачу журналов событий безопасности в т.ч. событий, связанных с работой датчиков вскрытия, неуспешных попыток идентификации/аутентификации;</p> <p>– события безопасности автоматически передаются в систему мониторинга, на основании которых формируется инцидент безопасности о компрометации ключей. Административный персонал в соответствии с эксплуатационной документацией проводят действия по отзыву ключей в ключевом центре;</p> <p>– организационно определенный список лиц, имеющих право доступа к оборудованию;</p> <p>– коммуникационный шкаф обслуживает не более 750 ПУ⁴. Негативные последствия от реализации возможности – минимальные, высокая стоимость и сложность подготовки реализации возможности</p>
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Неактуально	<p>– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;</p> <p>– высокая стоимость и сложность подготовки реализации</p>
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФК, в том числе с использованием исходных текстов входящего в СФК прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Неактуально	Неактуально	<p>– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;</p> <p>– высокая стоимость и сложность подготовки реализации возможности</p>
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)			
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования	Неактуально	Неактуально	<p>– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;</p>

⁴ Согласно Базовой модели угроз безопасности информации в интеллектуальных системах учёта электрической энергии (мощности).

Номер	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак		Обоснование отсутствия
		Для СОД ИВК	Для СОД ИВКЭ	
	для реализации атак недокументированных (недекларированных) возможностей системного ПО			– оборудование ИВКЭ обслуживает не более 750 ПУ ⁵ . Негативные последствия от реализации возможности – минимальные, высокая стоимость и сложность подготовки реализации возможности
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФК	Неактуально	Неактуально	– не осуществляется обработка сведений, составляющих государственную тайну
4.3	возможность воздействовать на любые компоненты СКЗИ и СФК	Неактуально	Неактуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

⁵ Согласно Базовой модели угроз безопасности информации в интеллектуальных системах учёта электрической энергии (мощности).

5 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности управляющих воздействий, направленных на полное и (или) частичное ограничение режима потребления электрической энергии (приостановление или ограничение предоставления коммунальной услуги), а также возобновление подачи электрической энергии.

Реализация (возникновение) угроз безопасности информации может привести к:

- нарушению прав граждан;
- возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора;
- возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства.

Таким образом, виды рисков (ущербов), которые могут наступить от нарушения или прекращения основных процессов системы, можно разделить на три типа:

- ущерб физическому лицу;
- ущерб юридическому лицу (владельцу ИСУЭ);
- ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической сферах деятельности.

Возможные негативные последствия, которые могут наступить при реализации (возникновении) угроз, приведены в таблице 9.

Т а б л и ц а 9 – Виды рисков (ущерба) и негативные последствия от реализации УБИ

Тип угрозы	Виды риска (ущерба)	Возможные негативные последствия
1	Ущерб физическому лицу	<ul style="list-style-type: none"> – не предоставление гарантированных услуг (нарушение гражданских прав); – дополнительные финансовые расходы (например, в случае необоснованного увеличения тарифа); – угроза жизни и здоровью (например, если человек подключен к системе жизнеобеспечения); – утечка персональных данных
2	Ущерб юридическому лицу	<ul style="list-style-type: none"> – необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) для устранения последствий; – невозможность решения целевых задач (реализации функций) или снижение эффективности решения задач (реализации функций); – необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций); – принятие неправильных решений (например, при изменении тарифа у пользователя); – получение преимущества конкурирующими организациями; – привлечение к административной ответственности; – привлечение к уголовной ответственности (статья 274.1 Федерального закона от 26.07.2017 № 194-ФЗ «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»); – репутационные риски
3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической сферах деятельности	<ul style="list-style-type: none"> – ущерб в секторе электроэнергетики страны, прекращение или нарушение функционирования предприятия в части невыполнения возложенной на функции; – дестабилизации социальной и экономической ситуации в стране; – дестабилизации политической ситуации в стране с целью создания внутривнутриполитического кризиса; – срыв заключения международных договоров

6 ОПРЕДЕЛЕНИЕ КЛАССА СКЗИ

Определение классов СКЗИ для компонент ИСУЭ приведено в таблице 10.

Актуальные классы СКЗИ СОД ИВКЭ и СОД ИВК представлены в таблице 11.

С учетом возможностей нарушителей при создании способов, подготовке и проведении атак на каналах связи, выходящих за пределы КЗ, и физического доступа к техническим средствам, на которых реализованы СКЗИ и СФК, можно сделать следующие выводы:

1 Для обеспечения защищенного информационного взаимодействия между СОД ИВК и СОД ИВКЭ в СОД ИВК должны использоваться СКЗИ, обеспечивающие криптографическую защиту по классу КСЗ и выше.

2 Для обеспечения защищенного информационного взаимодействия между СОД ИВК и СОД ИВКЭ в СОД ИВКЭ должны использоваться СКЗИ, обеспечивающие криптографическую защиту по классу КСЗ и выше.

3 Для обеспечения защищенного информационного взаимодействия между сегментами СОД ИВК должны использоваться СКЗИ, обеспечивающие криптографическую защиту по классу КСЗ и выше.

4 Для обеспечения защищенного информационного взаимодействия между СОД ИВК и смежными системами должны использоваться СКЗИ, обеспечивающие криптографическую защиту по классу КСЗ и выше.

Т а б л и ц а 10 – Определение классов СКЗИ

Номер	Возможности нарушителя	СОД ИВК	СОД ИВКЭ
СКЗИ класса КС1			
1	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ	+	+
2	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ	+	+
3	Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (контролируемой зоны)	+	+
4	Проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: – внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; – внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФК	+	+
5	Проведение атак на этапе эксплуатации СКЗИ на: – ключевую, аутентифицирующую и парольную информацию СКЗИ; – программные компоненты СКЗИ; – аппаратные компоненты СКЗИ; – программные компоненты СФК, включая ПО BIOS; – аппаратные компоненты СФК; – данные, передаваемые по каналам связи; – иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом, применяемых в Узле доступа информационных технологий, аппаратных средств и ПО	+	+
6	Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об Узле доступа, в которой используется СКЗИ	+	+
7	Применение: – находящегося в свободном доступе или используемого за пределами контролируемой зоны ПО, включая программные компоненты Системы и СКЗИ; – специально разработанного ПО	+	+

Номер	Возможности нарушителя	СОД ИВК	СОД ИВКЭ
8	Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: – каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами; – каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФК	+	+
9	Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети	+	+
10	Использование на этапе эксплуатации находящихся за пределами контролируемой зоны средства вычислительной техники (СВТ) и ПО из состава средств Системы, применяемых на местах эксплуатации СКЗИ (штатные средства)	–	+
СКЗИ класса КС2			
11	Проведение атаки при нахождении в пределах контролируемой зоны	+	+
12	Проведение атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты СФК. Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФК	+	+
13	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы Системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФК	+	+
14	Использование штатных средств, ограниченных мерами, реализованными в Узле доступа, в котором используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	–	–
СКЗИ класса КС3			
15	Физический доступ к СВТ, на которых реализованы СКЗИ и СФК	+	+
16	Возможность располагать аппаратными компонентами СКЗИ и СФК, ограниченная мерами, реализованными в Узле доступа, в котором используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	–	–
СКЗИ класса КВ			

Номер	Возможности нарушителя	СОД ИВК	СОД ИВКЭ
17	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФК, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	—	—
18	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в Узле доступа, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	—	—
19	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФК, в том числе с использованием исходных текстов входящего в СФК прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	—	—
СКЗИ класса КА			
20	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	—	—
21	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФК	—	—
22	Возможность располагать всеми аппаратными компонентами СКЗИ и СФК	—	—

Т а б л и ц а 11 – Классы СКЗИ

Номер	Тип средства	Класс	Возможности нарушителя	Комментарий
СОД ИВКЭ				
1	СКЗИ СОД ИВКЭ	не ниже КСЗ	<ul style="list-style-type: none"> – возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны с целью нарушения управляющих воздействий, направленных на осуществление ограничения режима потребления электрической энергии; – физический доступ к СВТ, на которых реализованы СКЗИ и СФК 	<p>Определен класс КСЗ, исходя из возможностей нарушителя:</p> <ul style="list-style-type: none"> – на каналах связи; – по физическому доступу к техническим средствам ИВКЭ, на которых реализованы СКЗИ и СФК.
СОД ИВК				
2	СКЗИ СОД ИВК	не ниже КСЗ	<ul style="list-style-type: none"> – возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны с целью нарушения управляющих воздействий, направленных на осуществление ограничения режима потребления электрической энергии; – проведение атаки при нахождении в пределах контролируемой зоны с целью получения документации на СКЗИ и штатные средства СФК на этапе эксплуатации. – физический доступ к СВТ, на которых реализованы СКЗИ и СФК 	<p>Определен класс КСЗ, исходя из возможностей нарушителя:</p> <ul style="list-style-type: none"> – на каналах связи; – по физическому доступу к техническим средствам, на которых реализованы СКЗИ и СФК; – с учётом большого объема данных, получаемых/передаваемых от оборудования ИВКЭ
3	Средства управления СКЗИ	не ниже КСЗ	<ul style="list-style-type: none"> – возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны с целью использованием сведений обо всех сетях связи в составе ИС, работающих на едином криптографическом ключе; – проведение атаки при нахождении в пределах контролируемой зоны 	<p>Определен класс КСЗ, исходя из возможностей нарушителя:</p> <ul style="list-style-type: none"> – на каналах связи; – по физическому доступу к техническим средствам, на которых реализованы СКЗИ и СФК

ПРИЛОЖЕНИЕ А

(справочное)

Источники разработки

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

2 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

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

4 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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

6 Базовая модель угроз безопасности информации в интеллектуальных системах учёта электрической энергии (мощности), разработанная 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.

7 Методический документ «Методика оценки угроз безопасности информации», ФСТЭК России, 2021.

8 Приказ Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».

9 Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

10 Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

11 Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

12 Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

к базовой модели угроз безопасности информации
интеллектуальной системы учета электрической энергии

**ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ
КОМПОНЕНТАМИ
ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА
ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ
ВАРИАНТ 2**

Типовая модель угроз программных средств криптографической защиты информации, применяемых для защиты информационно-вычислительных комплексов электроустановки (устройств сбора и передачи данных) и приборов учета в интеллектуальных системах и средств учёта электрической энергии (мощности)

ОГЛАВЛЕНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ	10
1.1 Назначение типовой модели угроз.....	10
1.2 Цели разработки типовой модели угроз.....	10
1.3 Объекты защиты.....	11
1.4 Структура Модели угроз	12
2 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА И СРЕДЫ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЗАЩИТЫ И ЦЕЛЕЙ БЕЗОПАСНОСТИ	14
2.1 Среда функционирования объектов защиты информации	14
2.1.1 Структура ИСУЭ.....	14
2.1.2 Требования к компонентам ИСУЭ, образующим среду функционирования СКЗИ ПУ и УСПД	16
2.2 Устройства сбора и передачи данных и приборы учета, применяемые в ИСУЭ.....	26
2.3 Описание жизненного цикла ПУ, УСПД, СКЗИ ПУ и УСПД	28
3 МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ, СКЗИ УСПД И ПУ	30
3.1 Внешний нарушитель N_{ext}	30
3.2 Внутренний нарушитель N_{int}	32
4 МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД И ПУ	35
4.1 Состав и описание угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД.....	35
4.1.1 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе производства	35
4.1.2 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе передачи.....	36

4.1.3 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе ввода в эксплуатацию.....	36
4.1.4 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе эксплуатации	37
4.1.5 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе технического обслуживания и ремонта	40
4.1.6 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе утилизации.....	41
4.2 Методика анализа угроз информационной безопасности УСПД, ПУ, СКЗИ УСПД и ПУ	41
4.3 Классификация угроз информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ	42
4.4 Описание мер противодействия угрозам информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ	54
4.5 Оценка эффективности мер противодействия угрозам информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ	102
5 ЗАКЛЮЧЕНИЕ ОБ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ УСПД, ПУ и СКЗИ УСПД и ПУ	114
ПРИЛОЖЕНИЕ А (СПРАВОЧНОЕ) ИСТОЧНИКИ РАЗРАБОТКИ.....	126

СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
ИВК	–	информационно-вычислительный комплекс
ИВКЭ	–	информационно-вычислительный комплекс электроустановки
ИСУЭ	–	интеллектуальная система учёта электрической энергии (мощности)
ОВ	–	оценка влияния (этап допуска защищенного устройства к эксплуатации)
ОС	–	операционная система
ПО	–	программное обеспечение
ПУ	–	прибор учета электрической энергии (мощности)
СКЗИ	–	средства криптографической защиты информации
СФК	–	среда функционирования криптосредств
ТИ	–	тематические исследования (этап сертификации СКЗИ)
УСПД	–	устройство сбора и передачи данных
ЦОД	–	центр обработки данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей типовой модели угроз программных средств криптографической защиты информации, применяемых для защиты информационно-вычислительных комплексов электроустановки (ИВКЭ) (устройств сбора и передачи данных (УСПД)) и приборов учета электрической энергии (мощности) (ПУ) в интеллектуальных системах и средств учёта электрической энергии (мощности) используются следующие понятия и определения [1, 2, 5 – 9]:

аутентификация (*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 документом «Правила доступа к минимальному набору функций интеллектуального учета электрической энергии (мощности)», утвержденным постановлением Правительства Российской Федерации от 19.06.2020 № 890, субъектам электроэнергетики и потребителям электрической энергии, в отношении которых они обеспечивают коммерческий учет электрической энергии.

доступность: свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

интеллектуальная система учета электрической энергии (мощности), ИСУЭ: 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.

информационно-вычислительный комплекс, ИВК: Совокупность технических средств, обеспечивающих автоматизированный сбор и хранение результатов измерений; контроль достоверности результатов измерений; диагностику состояния средств и объектов измерений; представление результатов измерений; формирование балансов электрической энергии на заданный период по всем балансовым группам; отключение (включение), ограничение предельной мощности нагрузки потребителей; осуществление коррекции хода часов элементов ИСУЭ и двусторонний обмен информацией между ИВКЭ, информационно-измерительными комплексами и ИВК и смежными системами.

информационно-вычислительный комплекс электроустановки, ИВКЭ: Совокупность технических средств, обеспечивающих автоматический сбор информации по учету электрической энергии от приборов учета, информации о состоянии средств измерений и двусторонний обмен информацией между ИВКЭ, информационно-измерительными комплексами и ИВК. В рамках настоящей Модели угроз может также использоваться, как синоним ИВКЭ, понятие «Устройство сбора и передачи данных».

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.

конфиденциальность: свойство, позволяющее не давать права на доступ к информации или не раскрывать ее полномочным лицам, логическим объектам или процессам.

криптоанализ: анализ криптографической системы и/или ее входов и выходов с целью получения конфиденциальных переменных и/или чувствительных данных, включая открытый текст.

криптографическая защита информации: защита информации с помощью ее криптографического преобразования.

модель угроз (безопасности информации): физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

нарушение информационной безопасности организации: случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

нарушитель информационной безопасности организации: физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

объект защиты информации: Информация или носитель информации или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

пароль (также транспортный секрет): конфиденциальная информация аутентификации, обычно состоящая из строки знаков.

прибор учета электрической энергии (мощности), ПУ: Измерительное устройство, присоединяемое к интеллектуальной системе учета, соответствующее требованиям постановления Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации» и постановления Правительства Российской Федерации от 19.06.2020 № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)».

программное обеспечение автоматизированной системы,
программное обеспечение АС: Совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС.

сертификация на соответствие: форма осуществляемого федеральным органом власти, уполномоченным в области безопасности, подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

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

управление доступом: Предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение использования ресурса неуполномоченным способом.

учетность (подотчетность): свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

целостность данных: способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа.

физическая защита информации: защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

шифрование: криптографическое преобразование данных (см. криптография) для получения шифротекста.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 НАЗНАЧЕНИЕ ТИПОВОЙ МОДЕЛИ УГРОЗ

Настоящая Модель угроз программных средств криптографической защиты информации, применяемых для защиты ИВКЭ (УСПД) и ПУ в интеллектуальных системах и средств учёта электрической энергии (мощности), требования к которым определяются Федеральным Законом Российской Федерации [1] и постановлением Правительства Российской Федерации [2] (далее – Модель угроз) разработана по поручению Минэнерго России (протокол совещания у заместителя директора Департамента развития электроэнергетики Минэнерго России Г. Э. Попова по вопросу возможности использования сетевыми организациями и гарантирующими поставщиками типовых частных моделей угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности) № 07-1898пр от 06.12.2023) и пункта 6 Положения о разработке шифровальных (криптографических) средств защиты информации [3] для постановки задач защиты информации и определения требований безопасности, предъявляемых к данным, среде функционирования криптосредств (СФК) и к средствам криптографической защиты информации (СКЗИ) ПУ и УСПД, применяемых в сетях владельца ИСУЭ.

1.2 ЦЕЛИ РАЗРАБОТКИ ТИПОВОЙ МОДЕЛИ УГРОЗ

Основными целями разработки настоящей Модели угроз являются:

– изучение состава объектов защиты, угроз информационной безопасности, возможностей нарушителей информационной безопасности СКЗИ УСПД и ПУ;

- определение уровня защищенности объектов защиты, а также состав функций (механизмов) информационной безопасности СКЗИ, которые должны обеспечить компенсацию угроз (обработку рисков) информационной безопасности УСПД и ПУ на всех этапах их жизненного цикла;
- оценка эффективности предлагаемых средств (мер, механизмов) информационной безопасности СКЗИ УСПД и ПУ.

1.3 ОБЪЕКТЫ ЗАЩИТЫ

Объектами защиты, к которым адресована настоящая Модель угроз, являются:

- команды управления энергопотреблением¹, формируемые информационно-вычислительным комплексом (ИВК) интеллектуальной системы учёта электрической энергии (мощности) (ИСУЭ), передаваемые на исполнительные органы управления энергопотреблением, находящиеся в составе УСПД и ПУ;
- команды, изменяющие режимы функционирования и настройки УСПД и ПУ;
- команды, изменяющие режимы функционирования и настройки УСПД и ПУ;
- показания приборов, служебная информация ИСУЭ, содержание выделенных (критичных) информационных обменов между ПУ/УСПД и ИВК;
- программное обеспечение (ПО) СКЗИ, данные, определяющие режимы функционирования СКЗИ, средства управления СКЗИ;
- ключевая информация СКЗИ;

¹ К командам управления энергопотреблением следует относить как команды, прямо изменяющие режим управления нагрузкой на реле прибора учета, исполняющего функцию управления нагрузкой, так и команды, в результате исполнения которых может быть казано негативное влияние на исполнения команд, прямо изменяющих режим управления нагрузкой. Состав таких команд должен быть определен индивидуально для каждой модели прибора разработчиком и представлен в документах, разрабатываемых им для оценки влияния конкретного прибора на СКЗИ.

- некриптографические секреты (в том числе транспортные), атрибуты идентификации и аутентификации (в том числе заводские номера ПУ и УСПД и номера СКЗИ);
- среда функционирования СКЗИ, включающая операционные системы (при наличии), ПО ПУ и УСПД, средства загрузки и обновления ПО СКЗИ и прочего ПО в составе СФК ПУ и УСПД, средства контроля целостности СФК СКЗИ ПУ и УСПД (в части, прошедшей оценку влияния);
- «Контролируемая зона» СКЗИ внутри корпуса ПУ и средства ее организации, защитные системы контролируемой зоны СКЗИ и сигналы (сведения) об изменении состояния контролируемой зоны;
- технические средства производства ПУ и УСПД, СКЗИ ПУ и УСПД, встраивания СКЗИ, ввода ключевой информации и некриптографических секретов, ввода ПУ, УСПД и работающих внутри них СКЗИ в эксплуатацию и контроля защищенности СФК СКЗИ в процессе эксплуатации;
- развернутая характеристика перечисленных объектов защиты приводится ниже в соответствующих разделах Модели угроз.

1.4 СТРУКТУРА МОДЕЛИ УГРОЗ

Типовая модель угроз программных средств криптографической защиты информации, применяемых для защиты ИВКЭ (УСПД) и ПУ в интеллектуальных системах и средств учёта электрической энергии (мощности) состоит из пяти частей:

- «Общие положения». Определяют назначение, статус документа и понятийный аппарат модели угроз;
- «Описание объектов защиты и целей безопасности». Включает описание объектов защиты, их взаимосвязей, жизненного цикла и прочих факторов, оказывающих влияние на состояние их информационной безопасности;

– «Модель нарушителя информационной безопасности УСПД и ПУ и СКЗИ УСПД и ПУ». Классификация нарушителей безопасности ПУ и УСПД и их возможностей (потенциала);

– «Модель угроз информационной безопасности УСПД и ПУ». Включает классификацию, состав, анализ угроз информационной безопасности УСПД, ПУ, СКЗИ УСПД и ПУ, а также мер противодействия угрозам безопасности (включая оценку эффективности мер противодействия);

– «Заключение об эффективности мер защиты УСПД, ПУ и СКЗИ УСПД и ПУ». Содержит основания для разработки СКЗИ УСПД и ПУ.

Методика анализа угроз и мер противодействия угрозам информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ включает четыре обобщенных этапа:

– описание угроз информационной безопасности применительно к каждому из видов объектов защиты с детализацией до уровня атак и характеристик атак, реализующих эти угрозы;

– выработка рекомендаций по выбору и применению средств защиты, общая классификация средств защиты от угроз информационной безопасности;

– оценка эффективности мер защиты и оценка остаточных рисков применительно к рассматриваемому комплексу угроз информационной безопасности;

– формирование заключения об эффективности мер защиты, в том числе резюме по результатам анализа, выполненного при разработке типовой модели угроз информационной безопасности.

2 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА И СРЕДЫ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЗАЩИТЫ И ЦЕЛЕЙ БЕЗОПАСНОСТИ

2.1 СРЕДА ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1.1 Структура ИСУЭ

Федеральный закон № 35-ФЗ [1] и постановление Правительства Российской Федерации № 890 [2] относят к интеллектуальным системам учета электрической энергии, включающим ИВК и ИВКЭ, но не относят к ИСУЭ приборы учета.

По определению [1] «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».

ПУ присоединяются к ИСУЭ через ИВКЭ/УСПД (для групповых объектов) или непосредственно (для уединенных объектов) и, в терминах [1], составной частью ИСУЭ не являются.

Для ИСУЭ в соответствии с требованиями [2] разработан проект Базовой модели угроз ИСУЭ [3]. Настоящая типовая Модель угроз разработана в соответствии с положениями и по прямому требованию Базовой модели угроз.

Обобщенная схема функциональной структуры среды функционирования СКЗИ ПУ и УСПД показана на рисунке 1.

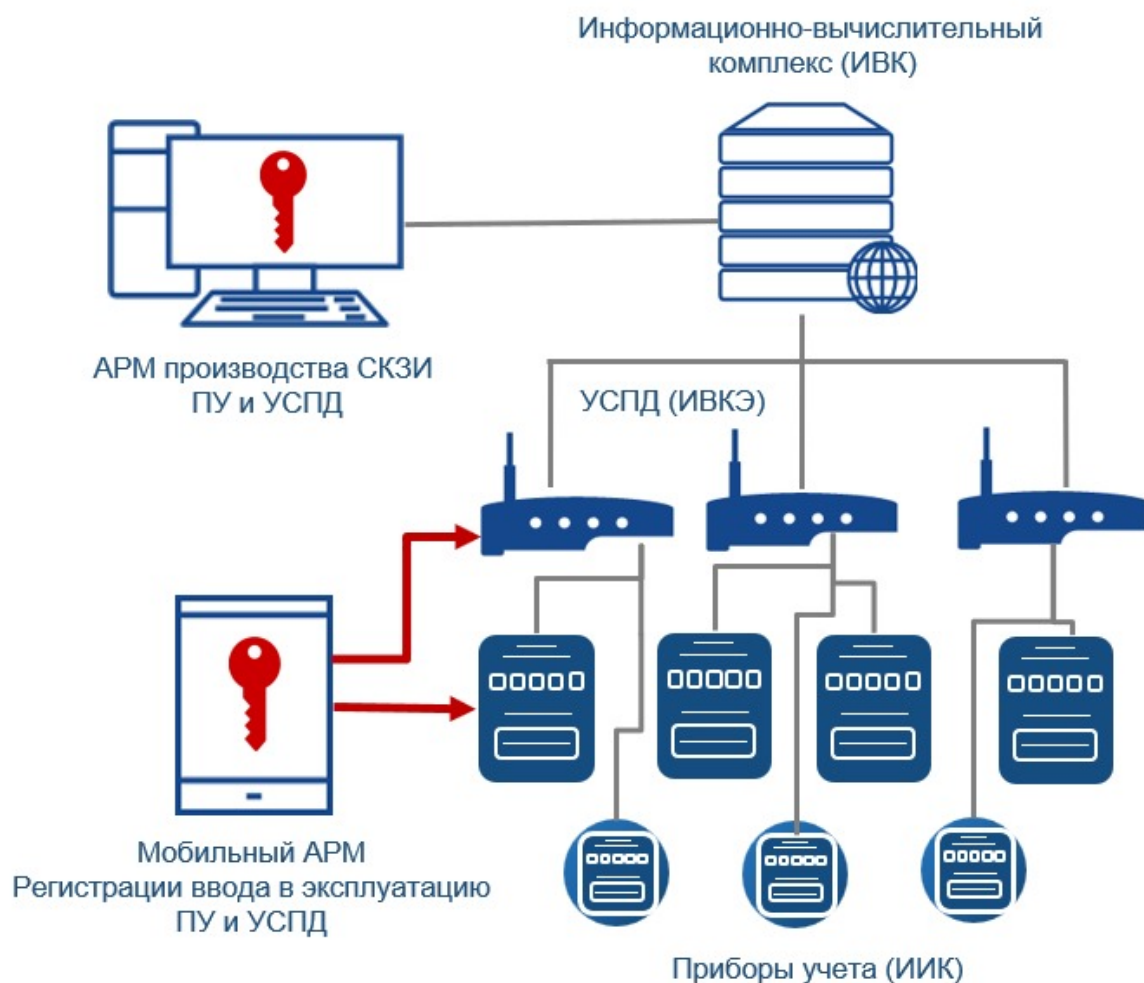


Рисунок 1 – Обобщенная схема функциональной структуры среды функционирования СКЗИ ПУ и УСПД

ИВК ИСУЭ обеспечивает управление, сбор показаний измерений и непрерывный мониторинг работоспособности ПУ и УСПД.

ИВКЭ (УСПД) применяется на уровне группового объекта (в типичном случае – многоквартирного жилого дома или отдельного подъезда) для обеспечения связи между приборами учета и ИВК и для ретрансляции команд управления от ИВК к ПУ. Как правило, зона применения подсети приборов учета, защищаемой УСПД, находится в зоне ограниченного доступа для посторонних лиц, монтируется в закрытых кабельных каналах и монтажных

шкафах, контролируется, наряду с пользователем ПУ и УСПД (сетевым оператором), потребителями электроэнергии и является достаточно защищенным локальным объектом, допускающим определенный уровень доверия к элементам данной подсети. Архитектура, в которой применяется УСПД, обычно именуется как «трехуровневая».

ПУ и УСПД взаимодействуют с ИВК, как правило, по открытым сетям передачи данных при помощи протоколов обмена информацией:

- по оптическим, проводным и беспроводным каналам связи с применением различных физических интерфейсов (Ethernet, RS-485, PLC, GSM (3G, 4G), ZigBee, NB-Fi) и протоколов канального уровня (PPP, RPoE, HDLC);
- транспортных протоколов TCP или UDP;
- стека протоколов DLMS/COSEM, российского отраслевого стандарта СПОДЭС [10].

В качестве компонентов среды функционирования ПУ и УСПД, кроме ИСУЭ, следует рассматривать средства производства ПУ и УСПД (включая средства/процессы встраивания СКЗИ и ввода некриптографических секретов), средства ввода в эксплуатацию (включая средства ввода ключевой информации), управления, технического обслуживания и ремонта.

2.1.2 Требования к компонентам ИСУЭ, образующим среду функционирования СКЗИ ПУ и УСПД

Требования к компонентам ИСУЭ системно проработаны в постановлении Правительства Российской Федерации [2]. В контексте настоящей Модели угроз существенными являются следующие требования [2]:

«28. Прибор учета электрической энергии, который может быть присоединен к интеллектуальной системе учета, должен удовлетворять требованиям, предъявляемым законодательством Российской Федерации об обеспечении единства измерений к средствам измерений, применяемым в

сфере государственного регулирования обеспечения единства измерений, и обеспечивать в точке учета:

в) ведение времени независимо от наличия напряжения в питающей сети с абсолютной погрешностью хода внутренних часов не более 5 секунд в сутки, а также с возможностью смены часового пояса;

г) возможность синхронизации и коррекции времени с внешним источником сигналов точного времени;

з) контроль наличия внешнего переменного и постоянного магнитного поля;

и) отображение на встроенном и (или) выносном цифровом дисплее: текущих даты и времени;

текущих значений потребленной электрической энергии суммарно и по тарифным зонам;

текущих значений активной и реактивной мощности, напряжения, тока и частоты;

значения потребленной электрической энергии на конец последнего программируемого расчетного периода суммарно и по тарифным зонам;

индикатора режима приема и отдачи электрической энергии;

индикатора факта нарушения индивидуальных параметров качества электроснабжения;

индикатора вскрытия электронных пломб на корпусе и клеммной крышке прибора учета электрической энергии;

индикатора факта события воздействия магнитных полей со значением модуля вектора магнитной индукции свыше 150 мТл (пиковое значение) на элементы прибора учета электрической энергии;

индикатора неработоспособности прибора учета электрической энергии вследствие аппаратного или программного сбоя;

<...>

л) индикацию функционирования (работоспособного состояния) на корпусе и выносном дисплее (при наличии выносного дисплея);

м) наличие 2 интерфейсов связи для организации канала связи (оптического и иного другого), а в отношении приборов учета электрической энергии трансформаторного включения также по цифровому электрическому интерфейсу связи RS-485 или цифровому электрическому интерфейсу связи Ethernet;

н) защиту прибора учета электрической энергии от несанкционированного доступа с помощью реализации в приборе учета:

идентификации и аутентификации;

контроля доступа;

контроля целостности;

регистрации событий безопасности в журнале событий;

о) фиксирование несанкционированного доступа к прибору учета посредством энергонезависимой электронной пломбы, фиксирующей вскрытие клеммной крышки и вскрытие корпуса (для разборных корпусов);

п) фиксацию воздействия постоянного или переменного магнитного поля с указанием даты и времени воздействия со значением модуля вектора магнитной индукции свыше 150 мТл (пиковое значение);

р) запись событий в отдельные выделенные сегменты энергонезависимой памяти прибора учета электрической энергии (с указанием даты и времени), результатов нарушения индивидуальных параметров качества электроснабжения - в отдельные выделенные сегменты энергонезависимой памяти прибора учета электрической энергии (далее соответственно - журнал событий, ведение журнала событий) в объеме не менее чем на 500 записей;

с) ведение журнала событий, в котором должно фиксироваться следующее:

дата и время вскрытия клеммной крышки;

дата и время вскрытия корпуса прибора учета электрической энергии (для разборных корпусов);

дата, время и причина включения и отключения встроенного коммутационного аппарата;

дата и время последнего перепрограммирования;

дата, время, тип и параметры выполненной команды;

попытка доступа с неуспешной идентификацией и (или) аутентификацией;

попытка доступа с нарушением правил управления доступом;

попытка несанкционированного нарушения целостности программного обеспечения и параметров;

изменение направления перетока мощности (для однофазных и трехфазных приборов учета электрической энергии);

дата и время воздействия постоянного или переменного магнитного поля со значением модуля вектора магнитной индукции свыше 150 мТл (пиковое значение) с визуализацией индикации;

факт связи с прибором учета электрической энергии, приведшей к изменению параметров конфигурации, режимов функционирования (в том числе введение полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии (управление нагрузкой);

дата и время отклонения напряжения в измерительных цепях от заданных пределов;

отсутствие или низкое напряжение при наличии тока в измерительных цепях с конфигурируемыми порогами (кроме однофазных и трехфазных приборов учета электрической энергии прямого включения);

отсутствие напряжения либо значение напряжения ниже запрограммированного порога по каждой фазе с фиксацией времени пропадания и восстановления напряжения;

инверсия фазы или нарушение чередования фаз (для трехфазных приборов учета электрической энергии);

превышение соотношения величин потребления активной и реактивной мощности;

небаланс тока в нулевом и фазном проводе (для однофазных приборов учета электрической энергии);

превышение заданного предела мощности;

т) формирование по результатам автоматической самодиагностики обобщенного события или каждого факта события;

у) изменение текущих значений времени и даты при синхронизации времени с фиксацией в журнале событий времени до и после коррекции или величины коррекции времени, на которую было скорректировано значение;

ф) возможность 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 (кроме приборов учета электрической энергии трансформаторного включения), в следующих случаях:

запрос интеллектуальной системы учета;

превышение заданных в приборе учета электрической энергии пределов параметров электрической сети;

превышение заданного в приборе учета электрической энергии предела электрической энергии (мощности);

несанкционированный доступ к прибору учета электрической энергии (вскрытие клеммной крышки, вскрытие корпуса (для разборных корпусов) и воздействие постоянным и переменным магнитным полем);

х) возобновление подачи электрической энергии по запросу интеллектуальной системы учета, в том числе путем фиксации встроенного коммутационного аппарата в положении "включено" непосредственно на приборе учета электрической энергии;

ш) обеспечение энергонезависимого хранения журнала событий, выявление фактов изменения (искажения) информации, влияющих на

информацию о количестве и иных параметрах электрической энергии, а также фактов изменения (искажения) программного обеспечения прибора учета электрической энергии;

щ) возможность организации с использованием защищенных протоколов передачи данных из состава протоколов, утвержденных Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с Министерством энергетики Российской Федерации, информационного обмена с интеллектуальной системой учета, в том числе передачи показаний, предоставления информации о результатах измерения количества и иных параметров электрической энергии, передачи журналов событий и данных о параметрах настройки, а также удаленного управления прибором учета электрической энергии, не влияющих на результаты выполняемых приборами учета электрической энергии измерений, включая:

корректировку текущей даты и (или) времени, часового пояса;

изменение тарифного расписания;

программирование состава и последовательности вывода сообщений и измеряемых параметров на дисплей;

программирование параметров фиксации индивидуальных параметров качества электроснабжения;

программирование даты начала расчетного периода;

программирование параметров срабатывания встроенных коммутационных аппаратов;

изменение паролей доступа к параметрам;

изменение ключей шифрования;

управление встроенным коммутационным аппаратом путем его фиксации в положении "отключено" (кроме приборов учета электрической энергии трансформаторного включения);

э) возможность передачи зарегистрированных событий в интеллектуальную систему учета по инициативе прибора учета электрической энергии в момент их возникновения и выбор их состава».

«29. Для приборов учета электрической энергии непосредственного включения необходимо наличие возможности физической (аппаратной) блокировки срабатывания встроенного коммутационного аппарата, используемого для полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии, приостановления или ограничения предоставления коммунальной услуги (управление нагрузкой). Реализация физической (аппаратной) блокировки должна сопровождаться процессом опломбирования».

«38. Защита интеллектуальной системы учета и содержащейся в ней информации должна обеспечиваться в соответствии с федеральными законами "О персональных данных", "О безопасности критической информационной инфраструктуры Российской Федерации", "Об информации, информационных технологиях и о защите информации" и актами Федеральной службы безопасности Российской Федерации, разработанными в соответствии с подпунктом "ш" статьи 13 Федерального закона "О федеральной службе безопасности", путем принятия организационных и технических мер, а также в соответствии с настоящими Правилами».

«39. Необходимость шифрования (применение средств криптографической защиты) информации при ее передаче по каналам связи интеллектуальной системы учета определяется субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, самостоятельно.

При определении субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, необходимости шифрования (применения средств криптографической защиты) информации при ее передаче по каналам связи интеллектуальной системы учета рекомендуется руководствоваться базовой моделью нарушителя (моделью угроз

безопасности информации), размещенной на официальном сайте Министерства энергетики Российской Федерации в информационно-телекоммуникационной сети "Интернет"».

«40. В целях определения актуальных угроз безопасности информации, обрабатываемой в интеллектуальных системах учета, субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, могут быть разработаны частные модели нарушителя (модели угроз безопасности информации).

При разработке частных моделей нарушителя (моделей угроз безопасности информации) рекомендуется использовать базовую модель нарушителя (модель угроз безопасности информации) в интеллектуальных системах учета, размещаемую на официальном сайте Министерства энергетики Российской Федерации в информационно-телекоммуникационной сети "Интернет"».

«41. В случае, когда субъектом электроэнергетики, являющимся владельцем интеллектуальной системы учета, определена потребность в криптографической защите информации, обрабатываемой в такой системе, рекомендуется применять средства криптографической защиты информации, прошедшие процедуру оценки соответствия требованиям, предъявляемым федеральным органом исполнительной власти в области обеспечения безопасности.

Сертифицированные средства защиты информации применяются в случаях, установленных законодательством Российской Федерации о техническом регулировании».

«42. Принимаемые меры по защите интеллектуальной системы учета и содержащейся в ней информации должны в том числе обеспечивать:

а) механизмы идентификации и аутентификации по логину и паролю в каждом из компонентов и элементов интеллектуальной системы учета с обязательной фиксацией в интеллектуальной системе учета информации о неверном вводе пароля;

б) предотвращение неправомерного доступа к информации, обрабатываемой и хранимой в интеллектуальной системе учета и приборах учета электрической энергии, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

в) недопущение воздействия на технические и программные средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование интеллектуальной системы учета;

г) восстановление функционирования интеллектуальной системы учета в том числе за счет резервирования информации и (или) технических средств обработки информации, каналов связи;

д) контроль доступа пользователей к данным и операциям в интеллектуальной системе учета;

е) своевременное обнаружение фактов несанкционированного доступа к интеллектуальной системе учета и содержащейся в ней информации».

«43. Прибор учета электрической энергии не должен иметь возможность управления ограничением нагрузки другими элементами интеллектуальной системы учета и другими приборами учета электрической энергии (не должен инициировать управляющие сигналы и воздействия)».

«44. Допускается ретрансляция одним прибором учета электрической энергии сигналов управления, полученных им с промежуточного элемента интеллектуальной системы учета и адресованных другим приборам учета электрической энергии, в случае его функционирования в режиме ретрансляции».

Данные требования были дополнительно разъяснены Министерством энергетики Российской Федерации в письме от 16.07.2021 № СП-8400/07 «Об СКЗИ для интеллектуальных систем учета электрической энергии», в котором, в частности говорится:

«...необходимо в состав типовых функциональных и эксплуатационных требований к СКЗИ включить следующие требования:

назначенный срок эксплуатации СКЗИ для ИВКЭ должен быть не менее 16 лет;

СКЗИ для ИВКЭ должны иметь непрерывно действующие сертификаты соответствия, выданные ФСБ России, в течение всего назначенного срока эксплуатации;

СКЗИ для ИВКЭ должны обеспечивать возможность дистанционного обновления их программного обеспечения, в том числе в целях их приведения в соответствие с новыми требованиями по безопасности информации, которые могут быть приняты в течение их назначенного срока эксплуатации;

СКЗИ для ИВКЭ должны обеспечивать возможность дистанционного обновления программного обеспечения ИВКЭ;

для эксплуатации СКЗИ для ИВКЭ не требуется создания контролируемой зоны, выходящей за пределы корпуса ИВКЭ, подлежащих защите с использованием СКЗИ, а также дополнительных средств контроля доступа в составе СКЗИ для ИВКЭ, помимо предусмотренных Правилам предоставления доступа к ИСУ;

СКЗИ для ИВКЭ не должны требовать особых условий размещения на объектах потребителей;

в правилах пользования СКЗИ должен быть разработан сценарий действий владельца ИСУ в случае компрометации ключа шифрования СКЗИ для ИВКЭ в момент эксплуатации, не приводящий к кардинальной замене всего оборудования ИСУ;

СКЗИ для ИВКЭ должны обеспечивать возможность их эксплуатации без необходимости физического доступа к ним, в том числе без замены их аппаратных частей, в течение всего назначенного срока эксплуатации;

СКЗИ для ИВКЭ должны обеспечивать совместимость всех экземпляров изделий, подключенных к ИСУ, независимо от объекта их размещения;

СКЗИ для ИВКЭ должны обеспечивать совместимость с программно-аппаратными средствами, применяемыми в элементах ИСУ, подлежащих защите с использованием СКЗИ;

встраивание СКЗИ для ИВКЭ должно нести минимальные издержки по времени и затратам для производителей ИВКЭ и не должно оказывать существенного влияния на технологический процесс производства;

СКЗИ, предназначенные для использования в составе ИСУ, должны быть совместимы с программно-аппаратными средствами действующих ИСУ;

в СКЗИ должна быть реализована и функция шифрования, и функция электронной подписи;

СКЗИ не должны предъявлять дополнительные требования к персоналу;

СКЗИ для ИВКЭ должно быть реализовано в виде аппаратного средства СКЗИ или в виде программного обеспечения СКЗИ.

Кроме того, необходимо в состав типовых функциональных и эксплуатационных требований к СКЗИ рассмотреть возможность включения требований по дистанционной загрузке ключей в СКЗИ для ИВКЭ после их установки на объекте потребителя, а также дистанционного обновления ключей в СКЗИ для ИВКЭ в течение всего назначенного срока эксплуатации».

«Одновременно полагаем целесообразным рассмотреть возможность предъявления к СКЗИ для ИСУ таких требований по безопасности информации, при которых деятельность по разработке и производству элементов ИСУ, подлежащих защите с использованием СКЗИ, а также деятельность по их установке и ремонту на объектах потребителей могла бы осуществляться соответствующими организациями без необходимости получения лицензий на деятельность с шифровальными (криптографическими) средствами».

2.2 УСТРОЙСТВА СБОРА И ПЕРЕДАЧИ ДАННЫХ И ПРИБОРЫ УЧЕТА, ПРИМЕНЯЕМЫЕ В ИСУЭ

Устройства сбора и передачи данных, применяемые в ИСУЭ в типовом случае, представляют собой достаточно разнообразный по мощности, конструктивному исполнению и функционалу класс вычислительных систем, работающих на основе того или иного ядра операционной системы (ОС) Linux.

Приборы учета электрической энергии (мощности), применяемые в ИСУЭ в типовом случае представляют собой устройство на основе специализированного микроконтроллера, имеющего в своем составе датчики (аналогово-цифровые преобразователи) для изменения параметров электрической энергии (мощности) и встроенный коммутационный аппарат (реле), используемый для полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии, работающее без ОС.

Перечень типовых микроконтроллеров, применяемых в ПУ и УСПД, приведен в таблице 1.

Т а б л и ц а 1

Марка	Изготовитель	Ссылка на спецификацию
ПРИБОРЫ УЧЕТА		
Байкал-Т (ВЕ-Т1000)	Байкал Электроникс	https://www.baikalelectronics.ru/products/35/
Байкал-М (ВЕ^1000)	Байкал Электроникс	https://www.baikalelectronics.ru/products/238/
УСТРОЙСТВА СБОРА И ПЕРЕДАЧИ ДАННЫХ		
K1986BK025	Миландр	https://ic.milandr.ru/products/mikroskhemy_v_plastikovyy_korpusakh/k1986vk025-okr-schetchik-m-/#props-tab

Многие из перечисленных микроконтроллеров поддерживают встроенные функции безопасности:

- уникальной идентификации каждого устройства;

- загрузки и исполнения доверенного программного обеспечения;
- использования энергонезависимой памяти с однократной записью данных;
- использования защищенной энергонезависимой памяти с контролем доступа;
- изоляции вычислительных процессов;
- контролируемого ввода-вывода (обмена данными) для изолированных процессов.

2.3 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА ПУ, УСПД, СКЗИ ПУ И УСПД

Состав этапов жизненного цикла ПУ, УСПД, СКЗИ ПУ и УСПД приведен на рисунке 2.



Рисунок 2

На этапе производства выполняется сборка аппаратной платформы УСПД и (или) ПУ, прошивка программного обеспечения, встраивание СКЗИ, могут выполняться также прошивка криптографических ключей и (или) транспортных секретов (паролей).

На этапе передачи УСПД и ПУ могут выполняться транспортировка, хранение, неоднократная передача прав собственности на ПУ и УСПД.

На этапе установки ПУ (УСПД) выполняются распаковка, монтаж, коммутация, подключение к сетям энергоснабжения, подключение к ИВК, конфигурирование, установка физических мер защиты устройств, могут выполняться также ввод криптографических ключей и ключевых документов, управление политикой безопасности СКЗИ.

На этапе эксплуатации ПУ и УСПД могут выполняться операции измерения параметров учета электроэнергии, приема и

передачи данных, управления, в т.ч. режимами энергопотребления, управление СКЗИ, обновление программного обеспечения, включая программное обеспечение СКЗИ.

На этапе ремонта могут выполняться процедуры диагностики, восстановления работоспособности ПУ и УСПД, прошивки (обновления) программного обеспечения, включая программное обеспечение СКЗИ.

На этапе утилизации могут выполняться операции разборки, уничтожения ПУ и УСПД, в том числе - уничтожения СКЗИ, криптографических ключей и ключевых документов.

Угрозы СКЗИ ПУ и УСПД на различных этапах жизненного цикла отличаются друг от друга и требуют и применения различных мер информационной безопасности в зависимости от этапа жизненного цикла СКЗИ УСПД и ПУ.

3 МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ, СКЗИ УСПД И ПУ

В настоящей Модели угроз рассматриваются два вида нарушителей информационной безопасности объектов защиты:

- внешние нарушители (Next), получающие, преимущественно, сетевой доступ к объектам защиты информации;
- внутренние нарушители (Hint), сотрудники служб ввода в эксплуатацию и технического обслуживания (ремонта) ПУ и УСПД.

3.1 ВНЕШНИЙ НАРУШИТЕЛЬ N_{EXT}

В качестве внешних нарушителей, с точки зрения атаки на ПУ, УСПД, СКЗИ ПУ и УСПД могут выступать:

- потребители электрической энергии, операторы транспортных, складских и прочих услуг, не связанных с эксплуатацией и техническим обслуживанием ПУ и УСПД;
- пользователи сетей общего пользования, хакеры, криминальные элементы, пытающиеся методами сетевого доступа получить несанкционированный доступ к показаниям приборов учета, информационным обменам, командам управления, программному обеспечению, среде функционирования СКЗИ, СКЗИ, криптографическим ключам ПУ и УСПД.

В ряде случаев внешние нарушители, особенно имеющие криминальные мотивы, могут объединяться в значительные по численности и совокупному составу технических средств и материальных ресурсов преступные группировки и сообщества.

Мотивы нарушителя.

Внешний нарушитель Next может быть мотивирован любыми корыстными, криминальными, террористическими мотивами, мотивами промышленного шпионажа, или бескорыстными, вандальными или хакерскими, интересами.

Знания о системе защиты ИСУЭ, ПУ и УСПД.

Нарушители Next могут изучать техническую документацию УСПД и ПУ, приобретать оборудование, осуществлять исследования и модернизации отдельных образцов техники, могут привлекать к сотрудничеству, в том числе с применением методов социальной инженерии, квалифицированных профильных специалистов производителей ПУ и УСПД, служб технического обслуживания, бывших сотрудников профильных предприятий, ИСУЭ и т.п. По этим причинам нарушители Next могут обладать практически полными знаниями об отдельных образцах техники, протоколах передачи данных, содержании, способах формирования сообщений, включая команды управления энергопотреблением.

Возможности нарушителя.

Внешние нарушители Next могут пытаться осуществлять проникновение в автоматизированные системы и отдельные их узлы, вести разработку вредоносного программного обеспечения, компрометировать сетевые и вычислительные ресурсы третьих лиц, накапливать ресурсы бот-сетей, организовывать атаки для подавления услуг автоматизированных (информационных) систем.

Техническое вооружение и знания нарушителя.

Нарушитель Next вооружен средствами для осуществления сетевых атак (средства перехвата трафика на отдельных звеньях его передачи, средствами разведки топологии сети и сканирования портов, анализаторами протоколов и т.п.), средствами взлома аппаратных средств, средствами дизайна аппаратных средств, средствами разработки программного обеспечения. Кроме того, в распоряжении нарушителя Next могут находиться средства для проведения примитивного криптоанализа на ограниченных вычислительных мощностях.

Потенциал нарушителя Next должен оцениваться дифференцированно, в зависимости от способа доступа к объектам защиты:

а) при осуществлении атак методом непосредственного физического воздействия на материальные объекты (приборы учета, УСПД, технические средства помещаемые внутрь контролируемой зоны, формируемой при помощи защищенных корпусов этих устройств), потенциал нарушителя Next необходимо признать чрезвычайно низким:

- в силу низкого ущерба от атаки на единичный объект, большого количества (десятки миллионов ПУ и сотни тысяч УСПД) объектов, распределенных по обширным территориям, и, как следствие, практической невозможности нанесения физического ущерба для большого числа объектов;

- в силу контролируемости объектов, а именно - физически ограниченного доступа к местам установки оборудования (запираемые помещения с контролем доступа), постоянного контроля работы оборудования (мониторинга) со стороны ИВК;

- в силу поднадзорности выполнения работ на объектах при выполнении этих работ сервисными или эксплуатирующими организациями (физический доступ на подобные объекты выполняется только после подготовки плана работ, допуска к работам по распоряжению/наряду и инструктажа, а работы производятся под надзором ответственного за выполнение работ);

- в силу общественного надзора за местами установки приборов, прежде всего со стороны потребителей электрической энергии.

б) при осуществлении атак методами сетевого доступа потенциал нарушителя Next следует оценивать как средний, в случае, если исполнителем атаки является индивидуальный злоумышленник, и как высокий, в случае, если угроза исходит от организованного криминального или хакерского сообщества.

3.2 ВНУТРЕННИЙ НАРУШИТЕЛЬ N_{INT}

Ввиду проведения комплекса организационно-технических мер безопасности, в том числе описанных ниже, и мер работы с персоналом владельца ИСУЭ не рассматривает в качестве внутренних нарушителей сотрудников владельца ИСУЭ и дочерних зависимых обществ и в силу процедур контроля за параметрами функционирования и качеством применяемой в отрасли продукции считает практически нереализуемыми атаки со стороны производителей ПУ, УСПД и являющихся лицензиатами ФСБ России производителей СКЗИ ПУ и УСПД.

В рамках настоящей Модели угроз в качестве внутренних нарушителей Hint могут рассматриваться операторы сервиса ввода в эксплуатацию, технического обслуживания и ремонта ПУ и УСПД (за исключением складского, транспортного и т.п. сервисов, не имеющих доступа к контролируемым элементам программных и аппаратных систем внутри корпусов ПУ и УСПД).

Мотивы нарушителя.

Мотивы нарушителя Hint являются преимущественно корыстными, могут диктоваться, например, организацией услуг по изготовлению приборов учета, некорректно выполняющих измерения, занижающих показатели энергопотребления, сотрудничеством с потребителями электрической энергии, заинтересованными в занижении показаний потребления или тем или иным видом сотрудничества с нарушителями Next.

Возможности нарушителя.

Нарушители Hint могут обладать ограниченными финансовыми, материальными, техническими и производственными ресурсами.

Одновременно следует предполагать, что нарушители Hint при выполнении нелегальных операций рискуют своей занятостью, производственными договорами, лицензиями, и поэтому нелегальная деятельность в качестве нарушителя Hint крупных и экономически устойчивых предприятий или значительных по численности коллективов сотрудников таких предприятий маловероятна.

Техническое вооружение и знания нарушителя.

Техническое вооружение и знания нарушителя H_{int} изменяются от низкого (неквалифицированный сотрудник монтажной организации) до среднего, в отдельных случаях - до высокого уровня, соразмерного знаниям разработчика (производителя) ПУ и УСПД.

Потенциал нарушителя H^{\wedge} является, скорее, низким в силу ограниченности количества объектов защиты, которым данный нарушитель способен нанести ущерб.

4 МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД И ПУ

В настоящем разделе приводятся краткие (указанные в кавычках) и развернутые наименования угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, которые в дальнейшем анализе идентифицируются только сокращенными названиями и ссылкой на номер угрозы или способа ее реализации (атаки), присвоенный ей в настоящем разделе.

При использовании краткого именованя угроз из приведенного ниже перечня следует иметь в виду, что одноименные угрозы на различных этапах жизненного ПУ, УСПД, СКЗИ ПУ и УСПД могут иметь совершенно различный контекст, характеристики риска угрозы/атаки и могут компенсироваться совершенно различными методами.

4.1 СОСТАВ И ОПИСАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУ, УСПД, СКЗИ ПУ И УСПД

4.1.1 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе производства

На этапе производства могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.1.1, 4.1.1.2.

4.1.1.1 «Ошибка проектирования»: ошибка проектирования ПУ, УСПД, приводящая к появлению уязвимости технических средств и возможности реализации угроз информационной безопасности.

4.1.1.2 «Дефект, брак, недеklarированные возможности»: дефект или брак при производстве, недеklarированные возможности приборов, ошибка или нарушение при встраивании СКЗИ в ПУ или УСПД, приводящие к появлению уязвимости технических средств и возможности реализации угроз информационной безопасности.

4.1.2 Состав угроз информационной безопасности

ПУ, УСПД, СКЗИ ПУ и УСПД на этапе передачи

На этапе передачи продукции от предприятия-производителя до точки монтажа и подключения могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.2.1 – 4.1.2.3.

4.1.2.1 «Несанкционированный доступ, вскрытие»: несанкционированный доступ к приборам учета, УСПД и средствам их защиты, выполненный, в том числе, путем вскрытия упаковки и корпуса устройств, анализ архитектуры и технических решений, реверс-инжиниринг, копирование, дисассемблирование программного обеспечения, копирование некриптографических секретов и криптографических ключей (при их наличии). Сбор исходных данных для проектирования локальных (исполняемых путем физического вторжения) и дистанционных (исполняемых методами сетевого доступа) атак.

4.1.2.2 «Несанкционированная модернизация»: внесение несанкционированных изменений в конструкцию устройств или в программное обеспечение с целью отключения функций защиты информации и внесения уязвимостей, в том числе с использованием результатов атаки, указанной в пункте 4.1.2.1.

4.1.2.3 «Подмена, фальсификация»: изготовление функциональных аналогов или макетов ПУ и УСПД, не прошедших одобрение типа и оценку безопасности, с целями нарушения информационной безопасности ИСУЭ.

4.1.3 Состав угроз информационной безопасности

ПУ, УСПД, СКЗИ ПУ и УСПД на этапе ввода в эксплуатацию

На этапе ввода в эксплуатацию могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.3.1 – 4.1.3.2.

4.1.3.1 «Несанкционированная модернизация»: внесение несанкционированных изменений в конструкцию устройств или в ПО с целью отключения функций защиты информации и внесения уязвимостей, в том числе с использованием результатов атаки, указанной в пункте 4.1.2.1.

4.1.3.2 «Компрометация криптографических ключей устройства»: действия нарушителя с целями извлечения (чтения), нарушения конфиденциальности, нарушения целостности, подмены криптографических ключей и ключевых документов СКЗИ ПУ или УСПД.

4.1.4 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе эксплуатации

На этапе эксплуатации могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.4.1 – 4.1.4.19.

4.1.4.1 «Несанкционированная модернизация путем физического вмешательства в работу устройства»: внесение несанкционированных изменений в конструкцию ПУ и УСПД или в ПО ПУ и УСПД, выполняемое путем физического нарушения целостности устройства с целью отключения функций защиты информации и внесения уязвимостей, в том числе с использованием результатов атаки, указанной в пункте 4.1.2.1.

4.1.4.2 «Компрометация криптографических ключей устройства»: действия нарушителя с целями извлечения (чтения), нарушения конфиденциальности, нарушения целостности, подмены криптографических ключей и ключевых документов СКЗИ ПУ или УСПД.

4.1.4.3 «Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и УСПД»: перехват информационных обменов, нарушение целостности и конфиденциальности может выполняться в открытых сетях передачи данных, в радиоэфире, на узлах концентрации и ретрансляции данных и т. п. Может выполняться с целями и (или) включать искажение показаний приборов учета, искажение,

блокирование, перехват, повтор команд управления, вмешательства в процессы обновления программного обеспечения и т. п.

4.1.4.4 «Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и ПУ»: перехват информационных обменов, их анализ, несанкционированная модернизация, повтор сообщений, формирование ложных сообщений в обменах между ИВК и ПУ с целями:

- а) занижения показаний, передаваемых в ИВК;
- б) атак на систему управления энергопотреблением, подготовки атак, указанных в пунктах 4.1.4.6, 4.1.4.8, 4.1.4.10, 4.1.4.12, 4.1.4.16, 4.1.4.18, 4.1.4.19.

4.1.4.5 «Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между УСПД и ПУ»: перехват информационных обменов путем подключения к каналам связи между ПУ и УСПД и выполнение атак, подобных указанным в пунктах 4.1.4.3 и 4.1.4.4.

4.1.4.6 «Криптоанализ»: попытки дешифровать данные, восстановить ключи шифрования и аутентификации при перехвате трафика при взаимодействии устройств в составе ИСУЭ.

4.1.4.7 «Навязывание ложных партнеров по взаимодействию между ИВК и УСПД»: отключение или нарушение процессов аутентификации партнеров по взаимодействию, навязывание ложных партнеров по взаимодействию, выполняемое с целями реализации угроз, указанных в пунктах 4.1.4.10, 4.1.4.11, 4.1.4.12.

4.1.4.8 «Навязывание ложных партнеров по взаимодействию между ИВК и ПУ»: атака может выполняться путем различного рода проб и вмешательств и может использовать результаты выполнения атак, указанных в пунктах 4.1.4.2, 4.1.4.4, 4.1.4.6.

4.1.4.9 «Навязывание ложных партнеров по взаимодействию между УСПД и ПУ»: атака может выполняться путем нарушения системы коммутации электроцепей и информационных каналов в составе объекта, несанкционированных подключений, различного рода проб и вмешательств.

4.1.4.10 «Сетевое вторжение, несанкционированный доступ к ПУ»: несанкционированный доступ по сети к внутренним ресурсам и процессам ПУ, в результате которого могут быть выполнены атаки, указанные в пунктах 4.1.4.2, 4.1.4.6, 4.1.4.12, 4.1.4.14, 4.1.4.16.

4.1.4.11 «Сетевое вторжение, несанкционированный доступ к УСПД»: несанкционированный доступ по сети к внутренним ресурсам и процессам УСПД, в результате которого могут быть выполнены атаки, указанные в пунктах 4.1.4.2, 4.1.4.3, 4.1.4.6, 4.1.4.13, 4.1.4.15, 4.1.4.17.

4.1.4.12 «Внедрение вредоносного программного обеспечения в ПУ»: нарушение целостности ПУ, внедрение в ПО ПУ или СФК СКЗИ ПУ исполняемого кода, который может использоваться для выполнения атак, указанных в пунктах 4.1.4.2, 4.1.4.6, 4.1.4.14, 4.1.4.16.

4.1.4.13 «Внедрение вредоносного программного обеспечения в УСПД»: нарушение целостности УСПД, внедрение в ПО УСПД или СФК СКЗИ УСПД исполняемого кода, который может использоваться для выполнения атак, указанных в пунктах 4.1.4.2, 4.1.4.6, 4.1.4.15, 4.1.4.17.

4.1.4.14 «Перехват управления при взаимодействии ИВК и ПУ»: подача несанкционированных команд управления от имени ИВК на ПУ, в том числе с целями выполнения атак, указанных в пунктах 4.1.4.18, 4.1.4.19.

4.1.4.15 «Перехват управления при взаимодействии ИВК и УСПД»: подача несанкционированных команд управления от имени ИВК на УСПД, в том числе с целями выполнения атак, указанных в пунктах 4.1.4.18, 4.1.4.19.

4.1.4.16 «Несанкционированное применение локального конфигулятора ПУ»: подача несанкционированных команд управления от имени ИВК на ПУ с целями выполнения атак, указанных в пунктах 4.1.4.2, 4.1.4.6, 4.1.4.12, 4.1.4.14, 4.1.4.16, 4.1.4.18, 4.1.4.19.

4.1.4.17 «Несанкционированное применение локального конфигулятора УСПД»: подача несанкционированных команд управления от имени ИВК на УСПД с целями выполнения атак, указанных в пунктах 4.1.4.2, 4.1.4.6, 4.1.4.13, 4.1.4.15, 4.1.4.17, 4.1.4.18, 4.1.4.19.

4.1.4.18 «Атаки на инфраструктуру энергопотребления путем массовой компрометации ПУ и УСПД»: выполнение массового отключения потребителей от сетей энергоснабжения путем перехвата канала управления ИВК или путем компрометации массового парка ПУ и УСПД и накопления из компрометированных устройств бот-сети, нацеленной на массовую инфраструктурную атаку.

4.1.4.19 «Атаки на инфраструктуру энергопотребления со стороны компрометированного ПУ или УСПД»: выполнение массового отключения потребителей от сетей энергоснабжения путем несанкционированного доступа к управлению ИВК со стороны компрометированного ПУ или УСПД или со стороны несанкционированного устройства, подключенного к сети ПУ и УСПД. Атака может сочетаться с деструктивным воздействием на ИВК и (или) УСПД и ПУ для того, чтобы долгосрочно блокировать восстановление энергоснабжения потребителей.

4.1.5 Состав угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД на этапе технического обслуживания и ремонта

На этапе технического обслуживания и ремонта могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.5.1 и 4.1.5.2.

4.1.5.1 «Несанкционированная модернизация»: внесение в ходе ремонта уязвимости в аппаратную платформу или программное обеспечение с целями последующих атак на ПУ и УСПД.

4.1.5.2 «Компрометация криптографических ключей устройства»: считывание, запись криптографических ключей с целями их компрометации и использования для:

- а) занижения показаний, передаваемых в ИВК;
- б) атак на систему управления энергопотреблением.

4.1.6 Состав угроз информационной безопасности

ПУ, УСПД, СКЗИ ПУ и УСПД на этапе утилизации

На этапе утилизации могут реализоваться виды угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, указанные в пунктах 4.1.6.1 и 4.1.6.2.

4.1.6.1 «Несанкционированная модернизация»: подлежащие утилизации устройства могут модернизироваться с целями изготовления фальсифицированных устройств и выполнения атаки, указанной в пункте 4.1.2.3.

4.1.6.2 «Компрометация криптографических ключей устройства»: считывание криптографических ключей, накопление данных с целями выполнения атаки, указанной в пункте 4.1.4.6.

4.2 МЕТОДИКА АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ, СКЗИ УСПД И ПУ

Угрозы информационной безопасности реализуются путем различного рода атак.

Атака – метод осуществления заданной угрозы информационной безопасности определенным способом, реализованный нарушителем заданного класса. В рамках настоящего документа атаки характеризуются следующим набором данных:

- субъект, осуществляющий атаку (далее по тексту это нарушитель определенного типа, обладающий всеми доступными ему техническими средствами);

- объект (цель) атаки. Это целостность (Ц), доступность (Д), аутентичность (А), подотчетность (П), конфиденциальность (К) информационных активов в составе УСПД, ПУ и СКЗИ УСПД и ПУ;

- канал(ы) осуществления атаки.

Угрозы, реализуемые при помощи тех или иных атак, характеризуются различным уровнем риска реализации угрозы. Риск зависит от вероятности того, что состоится угрожающее событие, и от размера ущерба, который будет нанесен ИСУЭ в случае реализации угрожающего события [6], [8]. В настоящем документе будет принят метод качественного анализа, указанный ниже.

Применительно к определенной атаке риск и ущерб будут описываться тремя качественными значениями – высокий (В), средний (С), низкий (Н). В случае, когда остаточный риск будет характеризоваться исчезающе малыми значениями (например, риск компрометации стойкого криптографического ключа методом прямого перебора), будет применяться дополнительно характеристика «пренебрежимо малый» (П).

Оценка ущерба выполняется, как и для оценок риска, тремя значениями – высокий (В), средний (С), низкий (Н).

Взвешенная оценка риска атаки выполняется методом экспертной оценки на основе оценки ущербов, вероятности рискованных событий и вероятности успеха реализации атаки.

4.3 КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ И СКЗИ УСПД И ПУ

Классификация угроз информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ приведена в таблице 2.

Таблица 2

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ И УСПД НА ЭТАПЕ ПРОИЗВОДСТВА							
4.1.1.1	Ошибка проектирования	Ней	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Внесение уязвимости в аппаратную платформу или программное обеспечение в силу ошибки проектирования	С	С	Риск оценивается как средний в силу того, что уязвимость может носить массовый характер
4.1.1.2	Дефект, брак, недекларированные возможности	Ней	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Наличие трудно выявляемой уязвимости в аппаратной платформе или программном обеспечении вследствие отсутствия сведений об опасной функциональности	С	С	Риск оценивается как средний в силу того, что уязвимость может носить массовый характер
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ И УСПД НА ЭТАПЕ ПЕРЕДАЧИ							
4.1.2.1	Несанкционированный доступ, вскрытие	Нщ, Ней	ПУ, УСПД, СКЗИ ПУ и УСПД (Ц,Д,П)	Механическое или электромагнитное воздействие, вскрытие корпуса, разрушение защитных цепей систем физической защиты. Разведка с целями последующих атак на ПУ и УСПД	Н	Н	Ущерб оценивается как низкий, поскольку компрометация единичного устройства мало значима в масштабах ИСУЭ. Риск не оценивается как пренебрежимо малый, поскольку существует распространенная криминальная практика «предоставления услуг» по занижению показателей энергопотребления
4.1.2.2	Несанкционированная модернизация	Нщ, Ней	ПУ, УСПД, СКЗИ ПУ и УСПД (Ц,Д,П)	Внесение уязвимости в аппаратную платформу или программное обеспечение с целями последующих атак на ПУ и УСПД	Н	Н	Риск оценивается как низкий в силу того, что возможности нарушителя (и, следовательно, вероятность атаки) вне производственных условий

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							ограничены для выполнения в массовом порядке достаточно сложных технических операции
4.1.2.3	Подмена, фальсификация	Нш, ^хт	ПУ, УСПД, СКЗИ ПУ и УСПД (Ц,Д,П)	Подмена штатного изделия на иное, содержащее уязвимости, с целями последующих атак на ПУ и УСПД	С	С	Риск оценивается как средний, поскольку событие представляется маловероятным, однако подмена изделий не требует высоких трудозатрат от нарушителя
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ ВВОДА В ЭКСПЛУАТАЦИЮ							
4.1.3.1	Несанкционированная модернизация	Нш, ^хт	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Внесение уязвимости в аппаратную платформу или программное обеспечение с целями последующих атак на ПУ и УСПД	Н	С	Ущерб оценивается как низкий, поскольку компрометация единичного устройства мало значима в масштабах ИСУЭ. Риск оценивается как средний, поскольку существует распространенная криминальная практика «предоставления услуг» по занижению показателей энергопотребления, а этап жизненного цикла «ввод в эксплуатацию» является удобным для выполнения данной атаки
4.1.3.2	Компрометация криптографических ключей устройства	Нш, ^хт	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц)	Считывание, запись криптографических ключей с целями их компрометации и использования для (а) занижения показаний, передаваемых в ИВК или (б) атак на систему управления энергопотреблением	Н	С	Ущерб оценивается как низкий, поскольку компрометация единичного устройства мало значима в масштабах ИСУЭ. Риск оценивается как средний, поскольку существует распространенная криминальная практика «предоставления услуг» по занижению показателей энергопотребления, а этап

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							жизненного цикла «ввод в эксплуатацию» является удобным для выполнения данной атаки
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ И УСПД НА ЭТАПЕ ЭКСПЛУАТАЦИИ							
4.1.4.1	Несанкционированная модернизация путем физического вмешательства в работу устройства	Нш, ^xt	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Внесение уязвимости в аппаратную платформу или программное обеспечение путем физического нарушения целостности ПУ и УСПД с целями последующих атак на ПУ и УСПД	Н	П	Ущерб оценивается как низкий поскольку компрометация единичного устройства мало значима в масштабах ИСУЭ. Риск физического вмешательства в работу прибора учета или УСПД представляется пренебрежимо малым по той причине, что процесс физического внедрения трудоемок, требует применения инструментальных средств, выполняется в течение достаточно длительного времени, оставляет следы взлома и по всем перечисленным причинам связан с рисками обнаружения взломщика. Следует также учесть, что массовая реализация физических атак крайне маловероятна
4.1.4.2	Компрометация криптографических ключей устройства	^xt	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Считывание, запись криптографических ключей с целями их компрометации и использования для (а) занижения показаний, передаваемых в ИВК или (б) атак на систему управления энергопотреблением	С	С	Ущерб оценивается как средний, поскольку, несмотря на то, что компрометация единичного устройства мало значима в масштабах ИСУЭ, компрометация криптографических ключей может вести к компрометации ПУ и УСПД в массовых

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							масштабах и может способствовать успеху различных атак, включая радикальную угрозу реализации массированных атак 4.1.4.18, 4.1.4.19. Вместе с тем риск не оценивается как высокий, поскольку компрометация ключей единичного ПУ или УСПД не приводит автоматически к компрометации ключей ИВК
4.1.4.3	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и УСПД		УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Перехват, анализ, несанкционированная модернизация, повтор сообщений, формирование ложных сообщений в обменах между ИВК и УСПД с целями (а) занижения показаний, передаваемых в ИВК, (б) атак на систему управления энергопотреблением, подготовки атак 4.1.4.7, 4.1.4.11, 4.1.7.13, 4.1.4.18, 4.1.4.19	С	В	Ущерб оценивается как средний, в силу того, что атака на инфраструктуру ИСУЭ при передаче открытого трафика в адрес ИВК может привести к нарушению процесса управления ИСУЭ и поражению ИВК. Риск оценивается как высокий, в силу многочисленности хакерских действий в открытых сетях общего пользования.
4.1.4.4	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и ПУ	Кext	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Перехват, анализ, несанкционированная модернизация, повтор сообщений, формирование ложных сообщений в обменах между ИВК и ПУ с целями (а) занижения показаний, передаваемых в ИВК, (б) атак на систему управления энергопотреблением, подготовки атак 4.1.4.6, 4.1.4.8,	С	В	Ущерб оценивается как средний, в силу того, что атака на инфраструктуру ИСУЭ при передаче открытого трафика в адрес ИВК может привести к нарушению процесса управления ИСУЭ и поражению ИВК. Риск оценивается как высокий в силу высокой численности ПУ и массового характера осуществления атаки

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
				4.1.4.10, 4.1.4.12, 4.1.4.16, 4.1.4.18, 4.1.4.19			
4.1.4.5	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между УСПД и ПУ	^xt	ПУ и УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Выполнение атак, подобных 4.1.4.3 и 4.1.4.4, путем подключения несанкционированных, в том числе специализированных для выполнения атаки на УСПД, инфраструктуру ИСУЭ и ИВК устройств, к каналам связи между ПУ и УСПД	С	С	Риск оценивается как средний, в силу того, что атака на инфраструктуру ИСУЭ из сети, защищенной УСПД, может привести к значительному (оценен, как средний) ущербу, однако процесс подключения трудоемок, требует применения инструментальных средств, выполняется в течение достаточно длительного времени, как правило, в условиях надзора со стороны потребителей электроэнергии, оставляет следы взлома и по всем перечисленным причинам связан с рисками обнаружения взломщика. Следует также учесть, что массовая реализация физических атак крайне маловероятна
4.1.4.6	Криптоанализ	^xt	ПУ и УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Атака 4.1.4.6 требует предварительного накопления информационного материала путем выполнения атак 4.1.4.4 и 4.1.4.5. Атака осуществляется путем анализа контекстов открытой информации и шифротекстов с сопутствующей математической обработкой результатов	В	С	Ущерб от реализации атаки компрометации единичного ПУ и УСПД был оценен выше (4.1.4.2), как средний. Ввиду того, что в настоящее время повсеместно используются открытые обмены информацией между ПУ и ИВК, УСПД и ИВК или применяются не сертифицированные, не прошедшие оценку стойкости защиты, СКЗИ, риск успешного криптоанализа необходимо считать средним даже для

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							обладающего ограниченными ресурсами хакера
4.1.4.7	Навязывание ложных партнеров по взаимодействию между ИВК и УСПД	^xt	УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Атака может выполняться путем различного рода проб и вмешательств и может использовать результаты выполнения атак 4.1.4.2, 4.1.4.3, 4.1.4.6	С	В	Ущерб от компрометации единичного УСПД можно оценивать, как низкий или средний для устройств. Однако риск от реализации атаки 4.1.4.7 следует оценивать, как высокий по той причине, что сетевая атака данного типа может быть легко масштабирована, количество компрометированных устройств может оказаться большим и бот- сеть компрометированных УСПД может способствовать успеху различных атак, включая радикальную угрозу реализации массированных атак 4.1.4.18, 4.1.4.19. В последнем случае особый риск составляет подмена УСПД специализированным устройством, способным вести наблюдение за ИВК, делать предпринимать попытки несанкционированного доступа к ИВК и перехвата прав управления ИВК
4.1.4.8	Навязывание ложных партнеров по взаимодействию между ИВК и ПУ	^xt	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Атака может выполняться путем различного рода проб и вмешательств и может использовать результаты выполнения атак 4.1.4.2, 4.1.4.4, 4.1.4.6	Н	В	Ущерб от компрометации единичного ПУ пренебрежимо мал, однако риск от реализации атаки 4.1.4.8 следует оценивать, как высокий по той причине, что сетевая атака данного типа может быть легко масштабирована, количество компрометированных ПУ может оказаться большим и

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							бот-сеть компрометированных ПУ может способствовать успеху различных атак, включая радикальную угрозу реализации массированных атак 4.1.4.18, 4.1.4.19. В последнем случае особый риск составляет подмена прибора учета специализированным устройством, способным вести наблюдение за ИВК, предпринимать попытки несанкционированного доступа к ИВК и перехвата прав управления ИВК
4.1.4.9	Навязывание ложных партнеров по взаимодействию между УСПД и ПУ	^xt	ПУ и УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Атака может выполняться путем нарушения системы коммутации электроцепей и информационных каналов в составе объекта, несанкционированных подключений, различного рода проб и вмешательств	С	С	См. обоснование риска для атаки 4.1.4.5
4.1.4.10	Сетевое вторжение, несанкционированный доступ к ПУ	^xt	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа	Н	В	Оценка риска аналогична 4.1.4.8 по причине масштабируемости результатов атаки
4.1.4.11	Сетевое вторжение, несанкционированный доступ к УСПД	^xt	УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа	С	В	Оценка риска аналогична 4.1.4.7 по причине масштабируемости результатов атаки
4.1.4.12	Внедрение вредоносного	^xt	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа. Для приборов, не обладающих	Н	В	Оценка риска аналогична 4.1.4.8 по причине масштабируемости результатов атаки

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
	программного обеспечения в ПУ			сложной программной архитектурой, можно предполагать изготовление специализированных закладок и вирусов на основе исследований и реверс-инжиниринга конкретных образцов техники			
4.1.4.13	Внедрение вредоносного программного обеспечения в УСПД	^xt	УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа	С	В	Оценка риска аналогична 4.1.4.7 по причине масштабируемости результатов атаки
4.1.4.14	Перехват управления при взаимодействии ИВК и ПУ	^xt	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа, в том числе на основании результатов предварительно выполненных атак 4.1.4.2, 4.1.4.3, 4.1.4.6, 4.1.4.7, 4.1.4.11, 4.1.4.13	Н	В	Оценка риска аналогична 4.1.4.8 по причине масштабируемости результатов атаки
4.1.4.15	Перехват управления при взаимодействии ИВК и УСПД	^xt	УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Атака выполняется методами сетевого доступа, в том числе на основании результатов предварительно выполненных атак 4.1.4.2, 4.1.4.3, 4.1.4.6, 4.1.4.7, 4.1.4.11, 4.1.4.13	С	В	Оценка риска аналогична 4.1.4.7 по причине масштабируемости результатов атаки
4.1.4.16	Несанкционированное применение локального конфигуратора ПУ	^xt	ПУ, СКЗИ ПУ (А,К,Ц,Д,П)	Атака выполняется методами имперсонации, когда вместо устройства локального конфигурирования к ПУ подключается постороннее устройство или методами сетевого доступа к устройству локального конфигурирования ПУ	Н	Н	Ущерб от атаки оценивается как низкий, поскольку связан с единичным прибором учета. Риск от выполнения атаки низкий по причине ее ограниченной масштабируемости. Даже при условии массированного потока хакерских атак, целей атаки немного, они эксплуатируются в

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
							течение ограниченного времени и не всегда прямо связаны с ПУ и УСПД
4.1.4.17	Несанкционированное применение локального конфигуратора УСПД	^xt	УСПД, СКЗИ УСПД (А,К,Ц,Д,П)	Атака выполняется методами имперсонации, когда вместо устройства локального конфигурирования к УСПД подключается постороннее устройство или методами сетевого доступа к устройству локального конфигурирования УСПД	С	Н	Ущерб от атаки оценивается как низкий или средний, поскольку связан с единичным УСПД. Риск от выполнения атаки низкий по причине ее ограниченной масштабируемости. Даже при условии массированного потока хакерских атак, целей атаки немного, они эксплуатируются в течение ограниченного времени и не всегда прямо связаны с ПУ и УСПД
4.1.4.18	Атаки на инфраструктуру энергопотребления путем массовой компрометации ПУ и УСПД	^xt	ПУ и УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Атака может выполняться методами сетевого доступа к массовому парку ПУ и УСПД в случае компрометации криптографических ключей ИВК или иным путем (атаки 4.1.4.3-4.1.4.15), предоставляющим нарушителю Нс^ возможность накопить массированную бот-сеть из компрометированных ПУ и УСПД. Атака может сопровождаться деструктивным воздействием на ПУ и УСПД, затрудняющим восстановление энергоснабжения потребителей	В	В	Риск реализации угроз, выполняемых по типу инфраструктурных атак из класса 4.1.4.18, 4.1.4.19, связанных с массовыми нарушениями процесса энергоснабжения потребителей, оценивается как высокий; ущерб от реализации таких угроз чрезвычайно высок, сравним, а в ряде случаев может превосходить по техническим, экономическим, социальным и политическим последствиям, ущерб от крупных техногенных катастроф, экологических бедствий и террористических актов
4.1.4.19	Атаки на инфраструктуру	^xt	ИВК (А,К,Ц,Д,П),	Атака может выполняться методами сетевого доступа к ИВК со стороны	В	В	Риск оценивается как высокий по той причине, что компрометация приборов учета и (или) УСПД

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
	энергопотребления со стороны компрометированного ПУ или УСПД		ПУ и УСПД (А,К,Ц,Д)	компрометированного ПУ или УСПД или со стороны иного устройства, эмулирующего легитимный ПУ или УСПД. Атака может выполняться путем несанкционированного доступа, эксплуатации уязвимостей ИВК и имеет целью поэтапный захват прав доступа к ресурсам ИВК, прав оператора и (или) администратора ИВК. Атака может сопровождаться деструктивным воздействием на ИВК и, опосредованно, ПУ и УСПД, затрудняющим восстановление энергоснабжения потребителей			путем помещения в среду ПУ или УСПД вредоносного программного агента, или размещение в сети ПУ и УСПД постороннего вредоносного устройства, осуществляющего пробы несанкционированного доступа к ИВК с целями разведки уязвимостей ИВК и перехвата прав управления ИВК может привести к частичному или полному нарушению функций ИВК или к приобретению нарушителем прав доступа оператора или администратора ИВК. Последствия такой атаки могут привести к отключениям энергоснабжения в масштабах всей области управления ИВК, что, в свою очередь, может превосходить по техническим, экономическим, социальным и политическим последствиям, ущерб от крупных техногенных катастроф, экологических бедствий и террористических актов
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА							
4.1.5.1	Несанкционированная модернизация	Нш, ^хт	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Внесение в ходе ремонта уязвимости в аппаратную платформу или программное обеспечение с целями последующих атак на ПУ и УСПД	Н	С	Оценка риска аналогична 4.1.3.1

Номер пункта	Способ реализации угрозы (атака)	Описание атаки			Ущерб	Риск	Обоснование оценки риска
		Субъект	Объект	Канал			
4.1.5.2	Компрометация криптографических ключей устройства	H _{int} , H _{ext}	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц)	Считывание, запись криптографических ключей с целями их компрометации и использования для (а) занижения показаний, передаваемых в ИВК или (б) атак на систему управления энергопотреблением	Н	С	Оценка риска аналогична 4.1.3.2
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ УТИЛИЗАЦИИ							
4.1.6.1	Несанкционированная модернизация	H _{int} , H _{ext}	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц,Д,П)	Подлежащие утилизации устройства могут модернизироваться с целями изготовления фальсифицированных устройств и выполнения атаки 4.1.2.3	Н	С	Ущерб оценивается как низкий, поскольку компрометация единичного устройства мало значима в масштабах ИСУЭ. Риск оценивается как средний, поскольку существует распространенная криминальная практика «предоставления услуг» по занижению показателей энергопотребления, а этап утилизации ПУ и УСПД является удобным для выполнения данной атаки
4.1.6.2	Компрометация криптографических ключей устройства	H _{int} , H _{ext}	ПУ, УСПД, СКЗИ ПУ и УСПД (А,К,Ц)	Считывание криптографических ключей, накопление данных с целями выполнения атаки 4.1.4.6	Н	С	Ущерб оценивается как низкий, поскольку ценность подлежащих утилизации криптографических ключей невысока. Вместе с тем риск оценивается как средний, поскольку накопление таких ключей в массовых количествах весьма ценно для проведения эффективного криптоанализа 4.1.4.6

4.4 ОПИСАНИЕ МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ И СКЗИ УСПД И ПУ

Меры защиты от угроз информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ целесообразно классифицировать:

- по объекту защиты;
- по способу применения мер защиты;
- по отношению ко времени совершения угрожающего события.

Состав объектов защиты в настоящей Модели угроз представлен в подразделе 1.3, их детальное описание приведено в разделе 2.

По способу применения меры защиты (методов обработки риска) классифицируются как организационные, включая правовые (О), организационно-технические, сочетающие организационные мероприятия с применением технических средств (ОТ) и технические (Т), среди которых необходимо выделить криптографические (К) меры защиты данных.

По отношению ко времени совершения угрожающего события, меры обработки риска различают как проактивные (профилактические), применяемые для устранения причин возникновения риска до реализации угрожающего события, активные, оказывающие непосредственное противодействие угрожающим факторам в момент осуществления угрожающего события, и реактивные, применяемые после реализации угрожающего события.

В составе проактивных мер защиты должны быть выработаны и нормативно обоснованы требования к правилам работы с объектами защиты информации на всех этапах жизненного цикла УСПД, ПУ и СКЗИ УСПД и ПУ и требования по обеспечению информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ, указанные в таблице 3.

Т а б л и ц а 3

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
ПРОАКТИВНЫЕ МЕРЫ ЗАЩИТЫ				
П1	Классификация данных (включая содержание информационных обменов) ПУ, УСПД, СКЗИ ПУ и УСПД	О	Данные, передаваемые между ПУ и УСПД, ПУ и ИВК, УСПД и ИВК разделены по содержанию и по уровню критичности с точки зрения информационной безопасности на три класса: открытые данные, требования по защите не устанавливаются (тип соединения «Публичный клиент» в терминах [10]); показания приборов учета (тип соединения «Считывание показаний» в терминах [10]); команды управления компонентами ИСУЭ (тип соединения «Конфигуратор» в терминах [10]). В эту группу входят все команды коррекции времени, команды конфигурирования ПУ, УСПД и СКЗИ ПУ и УСПД, а также команды управления потреблением	
П2	Требования по защите данных ПУ, УСПД, СКЗИ ПУ и УСПД	О	Требования по защите данных [10] дифференцированы для различных типов соединений: – для соединения «Публичный клиент» требования не устанавливаются; – для соединения «Считывание показаний» устанавливаются	Ввиду того, что тонко гранулированный контроль доступа и фильтрация открытых данных при их передаче в защищенные информационные системы в ряде случаев может оказаться нерационально дорогой мерой защиты, допускается применение по

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			требования аутентификации источника данных и целостности; для соединения «Конфигуратор» устанавливаются требования аутентификации источника данных, целостности и конфиденциальности	отношению к открытым данным ИСУЭ мер избыточной защиты (шифрования)
П3	Требования по оценке стойкости СЗИ и СКЗИ	О	Для защиты приборов учета и УСПД должны применяться средства защиты информации, соответствующие требованиям отечественного технического регулирования, прошедшие в установленном порядке оценку стойкости защиты. В частности, СКЗИ должны быть разработаны в соответствии с требованиями Положения о разработке СКЗИ [4], а сами СКЗИ должны быть сертифицированы в системе ФСБ России	
П4	Регламенты применения средств защиты ПУ, УСПД, СКЗИ ПУ и УСПД	О	Правила применения средств защиты информации должны быть документированы и подлежат строгому исполнению. Правила пользования СКЗИ должны быть согласованы ФСБ России	
П5	Комплекс обязательных мер физической защиты и защиты информации ПУ, подключаемых к УСПД	ОТ	В соответствии с требованиями [2] для ПУ, подключаемых к ИВК через УСПД, должны применяться следующие меры физической защиты устройства:	Для ПУ, подключаемых к ИВК через УСПД, требования применения средств криптографической защиты информации устанавливаются, как рекомендательные, по тем

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>– энергонезависимое ведение времени;</p> <p>– возможность синхронизации и коррекции времени с внешним источником сигналов точного времени;</p> <p>– датчик внешних полей;</p> <p>– индикатор нарушения параметров электроснабжения;</p> <p>– энергонезависимой электронной пломбы (датчика вскрытия) корпуса и крышки клеммной коробки;</p> <p>– индикатор неработоспособности; возможность физической (аппаратной) блокировки срабатывания встроенного коммутационного аппарата;</p> <p>– реализация физической (аппаратной) блокировки должна сопровождаться процессом опломбирования.</p> <p>В соответствии с требованиями [2] для ПУ, подключаемых к ИВК через УСПД, должны применяться следующие меры защиты информации:</p> <p>– защита от несанкционированного доступа с помощью:</p> <p>– идентификации и аутентификации;</p> <p>– контроля доступа;</p> <p>– контроля целостности.</p>	<p>причинам, что такие ПУ эксплуатируются в зоне единого территориального объекта, используют локальные проводные соединения, как правило, со скрытым (защищенным) каналом прокладки кабелей и защищенным от несанкционированных перекоммутаций монтажом соединений и не подсоединены непосредственно к каналам (сетям) передачи данных общего пользования.</p> <p>Вместе с тем применение СКЗИ на приборах учета рекомендуется с целями:</p> <p>— защиты команд управления энергопотреблением при помощи электронной подписи ИВК (см. П18);</p> <p>– реализации тотальной защиты (изолирующей политики шифрования трафика) ПУ и УСПД (см. А9, А10)</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> – регистрация событий в журнале, содержащемся в защищенной энергонезависимой памяти; – автоматическая самодиагностика; – выявление фактов изменения (искажения) информации; – передача информации с использованием защищенных протоколов передачи данных; – передача зарегистрированных событий в момент их возникновения в ИВК по инициативе прибора учета; – своевременное обнаружение фактов несанкционированного доступа 	
П6	Комплекс обязательных мер физической защиты и защиты информации ПУ, подключаемых к ИВК	ОТ	<p>ПУ, подключаемые к ИВК, должны удовлетворять требованиям П5 и, кроме того, обеспечивать функции криптографической защиты информации, описанные в разделе П2, при передаче данных по открытым сетям передачи данных и по радиоканалам.</p> <p>Для ПУ, работающих на основе операционной системы, должны выполняться требования безопасности ОС, аналогичные требованиям П7, предъявляемым к ОС УСПД. Для ПУ, работающих без операционной системы, должны приниматься и контролироваться</p>	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			методы дизайна безопасной архитектуры сетевых взаимодействий (см. П35)	
П7	Комплекс обязательных мер физической защиты и защиты информации УСПД	ОТ	<p>К УСПД должны предъявляться требования [2], содержащиеся в разделе за исключением требований, присущих исключительно приборам учета.</p> <p>Для каждой модели УСПД, использующей операционную систему, должен быть составлен перечень присущих для данного типа ОС механизмов контроля доступа, контроля целостности ОС и прочих механизмов операционной безопасности, обязательных для применения при эксплуатации УСПД. Должно быть выполнено отключение всех не используемых при штатной эксплуатации УСПД приложений, служб операционной системы, должны быть закрыты все не используемые сетевые порты и отключены все сетевые соединения, кроме соединений с ИВК и доверенными серверами ИСУЭ. Для каждой модели УСПД, использующей операционную систему, должен быть составлен перечень встроенных в данную ОС и</p>	<p>Требование защиты клеммных коробок ПУ применительно к УСПД должно формулироваться как требование физической защиты узла коммутации УСПД, через который ПУ присоединяются к УСПД и УСПД присоединяется к ИВК. В качестве мер защиты могут применяться:</p> <ul style="list-style-type: none"> – защищенный корпус УСПД; – закрытый и опломбированный монтажный шкаф. <p>Средства физической защиты УСПД должны снабжаться электронным датчиком нарушения средств физической защиты.</p> <p>УСПД должно обеспечивать возможность физического отделения внутренней сети, предназначенной для связи с ПУ и внешней сети - для связи с ИВК (Центром управления сетями)</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>(или) выполненных в виде отдельных процессов (приложений, служб) механизмов сетевой информационной безопасности, включая средства межсетевого экранирования, безопасной (корпоративной) службы разрешения сетевых имен (DNS), средств защиты от вредоносного программного обеспечения, средств обнаружения вторжений, мониторинга, событийного протоколирования, сигнализации о тревожных событиях и прочих механизмов сетевой информационной безопасности, обязательных для применения при эксплуатации данной модели УСПД. Обновления ОС УСПД должны выполняться с доверенного сервера ИСУЭ. Прочие источники обновлений ПО УСПД и сетевые соединения, по которым такие обновления могут осуществляться, должны быть запрещены. Контроль перечисленных требований должен выполняться при оценке влияния УСПД на СКЗИ (ПЗ6)</p>	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П8	Требования к минимальному составу встроенных функций защиты информации аппаратной платформы ПУ	ОТ	<p>Аппаратная платформа ПУ должна обеспечивать на уровне микроконтроллера следующие механизмы безопасности:</p> <ul style="list-style-type: none"> - уникальный серийный номер или иное средство уникальной идентификации каждого устройства; -возможности привязки уникальных конфиденциальных данных к уникальному устройству; - поддержки безопасного процесса загрузки программного обеспечения, средства защиты начального загрузчика; - наличия защищенной энергонезависимой долговременной памяти с однократной записью данных; - наличия энергонезависимой долговременной памяти с многократными чтением и записью информации, защищенными при помощи пароля (некриптографического секрета); пароли на чтение, запись и удаление данных должны быть разделены; - наличия интерфейсов (контактных групп, портов и т.п. для подключения датчиков физической безопасности ПУ, описанных в требованиях П5 	Допускается применение аналогичных и (или) дополнительных механизмов безопасности в составе схемотехнического решения ПУ за пределами микроконтроллера. В частности, должны быть обеспечены механизмы электропитания цепей датчиков физической безопасности платформы ПУ

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П9	Требования к минимальному составу встроенных функций защиты информации аппаратной платформы УСПД	ОТ	К минимальному составу встроенных функций защиты информации аппаратной платформы УСПД предъявляются требования П8	Часть средств физической защиты УСПД может быть перенесена из контролируемой зоны внутри корпуса прибора в контролируемую зону в составе защищенного монтажного шкафа при условии не снижения общего уровня физической безопасности устройства. Для контроля безопасности УСПД могут дополнительно применяться датчики движения, датчики объема, средства видеонаблюдения и видеорегистрации
П10	Требования к УСПД по обеспечению безопасности взаимодействия между ПУ и ИВК (ПУ и УСПД)	ОТ	УСПД может ретранслировать для ПУ команды управления, получаемые от ИВК. В соответствии с требованиями [2], пункт 42а, каждый элемент ИСУЭ должен поддерживать механизмы идентификации и аутентификации по логину и паролю с обязательной фиксацией в интеллектуальной системе учета информации о неверном вводе пароля. С учетом данного требования каждый ПУ, подключаемый к ИСУЭ, должен обеспечивать: – возможности идентификации по уникальному серийному номеру и логическому имени;	Для ПУ, снабженных СКЗИ для взаимодействия с ИВК, данное требование не устанавливается. УСПД должно обеспечивать между ИВК и ПУ маршрутизацию сообщений, защищенных при помощи сквозного шифрования данных. При этом прямые взаимодействия между ПУ и УСПД (при наличии таких взаимодействий без участия ИВК) рекомендуется выполнять с применением криптографических функций аутентификации

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>– возможности аутентификации по паролю.</p> <p>Логин и пароль каждого устройства должны настраиваться с участием ИВК и резервироваться в базе данных ИВК.</p> <p>Данные требования должны выполняться для каждого ПУ и УСПД при каждом акте взаимодействия между ними.</p> <p>Рекомендуется применение, наряду с базовым логином и паролем, устанавливаемыми для прибора, применение одноразовых паролей для аутентификации устройств или применения средств аутентификации и контроля целостности сообщений при каждом взаимодействии между ПУ и УСПД или при сквозном взаимодействии между ПУ и ИВК. В случае, когда УСПД принимает от ИВК команду на управление энергопотреблением, адресованную определенному ПУ, подключенному к данному УСПД, СКЗИ УСПД должны:</p> <p>– для ПУ, не снабженных СКЗИ, выполнить проверку электронной подписи ИВК на команде управления (см. П18). Команда управления должна передаваться на ПУ только в</p>	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			случае положительного результата проверки электронной подписи ИВК –для ПУ, снабженных СКЗИ, - транслировать команду управления энергопотреблением в защищенном виде непосредственно к ПУ, исполняющему функции управления энергопотреблением	
П11	Требования к интеграции СКЗИ ПУ, подключаемых к ИВК при посредстве УСПД, со встроенными средствами физической защиты и защиты информации ПУ	ОТ	СКЗИ ПУ, подключаемых к УСПД, должны быть логически (программно, при помощи микроконтроллера и интерфейсов ПУ) интегрированы с сигналами датчиков нарушения физической безопасности ПУ и иметь возможность в реальном времени получать от датчиков сигналы о нарушениях физической безопасности устройства. Для ПУ, не снабженных СКЗИ, сведения о всяком событии нарушения физической безопасности ПУ должны немедленно передаваться в УСПД (для дальнейшей передачи в ИВК). Для ПУ, снабженных СКЗИ, сведения о всяком событии нарушения физической безопасности ПУ должны немедленно передаваться ИВК, после чего должны выполняться мера безопасности Р1	Конструктив ПУ должен обеспечивать возможность создания контролируемой зоны внутри защищенного от несанкционированного доступа корпуса прибора. Целостность периметра контролируемой зоны должна обеспечиваться как физическими (разрушаемые элементы корпуса, пломбы, наклейки и т.п.), так и логическими (датчики нарушения целостности конструкций и электрических цепей, датчики вскрытия, проникновения), срабатывающими при попытке несанкционированного доступа внутрь корпуса прибора. Данное требование устанавливается в целях реализации функций защиты П14 и Р1 и должно проверяться на этапе оценки влияния устройства на СКЗИ (П36)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			и, затем, P2. Дополнительно рекомендуется иметь в составе ПУ опциональные средства ввода сигналов от внешних датчиков безопасности внешнего периметра, например, датчиков несанкционированного вскрытия монтажного шкафа, помещения подстанции	
П12	Требования к интеграции СКЗИ ПУ, подключаемых непосредственно к ИВК, со встроенными средствами физической защиты и защиты информации ПУ	ОТ	СКЗИ ПУ, подключаемых к ИВК, должны быть логически (программно, при помощи микроконтроллера и интерфейсов ПУ) интегрированы с сигналами датчиков нарушения физической безопасности ПУ и иметь возможность в реальном времени получать от датчиков сигналы о нарушениях физической безопасности устройства. Сведения о всяком событии нарушения физической безопасности ПУ должны немедленно передаваться ИВК, после чего должны выполняться мера безопасности P1 и, затем, P2. Дополнительно рекомендуется иметь в составе ПУ опциональные средства ввода сигналов от внешних датчиков безопасности внешнего периметра, например, датчиков	Конструктив ПУ должен обеспечивать возможность создания контролируемой зоны внутри защищенного от несанкционированного доступа корпуса прибора. Целостность периметра контролируемой зоны должна обеспечиваться как физическими (разрушаемые элементы корпуса, пломбы, наклейки и т.п.), так и логическими (датчики нарушения целостности конструкций и электрических цепей, вскрытия, проникновения), срабатывающими при попытке несанкционированного доступа внутрь корпуса прибора. Данное требование устанавливается в целях реализации функций защиты П14 и P1 и должно проверяться на этапе оценки влияния устройства на СКЗИ (П36)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			несанкционированного вскрытия монтажного шкафа, помещения подстанции	
П13	Требования к интеграции СКЗИ УСПД со встроенными средствами физической защиты и защиты информации УСПД	ОТ	СКЗИ УСПД, должны быть логически (программно, при помощи микроконтроллера и интерфейсов УСПД) интегрированы с сигналами датчиков нарушения физической безопасности УСПД и иметь возможность в реальном времени получать от датчиков сигналы о нарушениях физической безопасности устройства. Сведения о всяком событии нарушения физической безопасности УСПД должны немедленно передаваться ИВК, после чего должны выполняться мера безопасности Р1 и, затем, Р2. Дополнительно, рекомендуется иметь в составе УСПД опциональные средства ввода сигналов от внешних датчиков безопасности внешнего периметра, например, датчиков несанкционированного вскрытия монтажного шкафа, помещения подстанции	Конструктив УСПД должен обеспечивать возможность создания контролируемой зоны внутри защищенного от несанкционированного доступа корпуса устройства. Целостность периметра контролируемой зоны должна обеспечиваться как физическими (разрушаемые элементы корпуса, пломбы, наклейки и т.п.), так и логическими (датчики нарушения целостности конструкций и электрических цепей, вскрытия, проникновения), срабатывающими при попытке несанкционированного доступа внутрь корпуса устройства. Применительно к УСПД допускается применение внешних дополнительных средств защиты для создания контролируемой зоны в периметре монтажного шкафа, в котором установлено УСПД. Данное требование устанавливается в целях реализации функций защиты П14 и Р1 и должно проверяться на этапе оценки влияния устройства на СКЗИ (П36)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П14	Требования на уничтожение криптографических ключей СКЗИ ПУ и УСПД при возникновении рисков (подозрительных) событий	ОТ	Криптографические ключи СКЗИ ПУ и УСПД должны уничтожаться в случае наступления рисков событий, минимальный перечень которых приведен в требовании П33. Должна быть также предусмотрена возможность уничтожения криптографических ключей ПУ (УСПД) по команде ИВК или доверенного сервера ИСУЭ	Перечень рисков событий ПУ и УСПД, приводящих к уничтожению криптографических ключей, должен быть включен в эксплуатационную документацию ПУ или УСПД. Выполнение требования П14 должно контролироваться при оценке влияния устройства на СКЗИ (П36)
П15	Требование обновления криптографических ключей	ОТ	Применение СКЗИ ПУ и УСПД в течение назначенного срока эксплуатации не должно ограничиваться сроком жизни криптографических ключей и ключевых документов. Выполнение требования автономной эксплуатации СКЗИ в течение назначенного срока эксплуатации устройств должно обеспечиваться за счет защищенного процесса обновления криптографических ключей и ключевых документов в процессе эксплуатации	
П16	Требование применения криптографических ключей с минимизированным сроком жизни	ОТ	Для снижения рисков, связанных с атаками 4.1.4.2, 4.1.4.6, 4.1.4.10, 4.1.4.11 сроки жизни криптографических ключей и ключевых документов должны быть рационально минимизированы. Минимальный срок эксплуатации	Срок жизни криптографических ключей, применяемых для защиты УСПД и ПУ, снабженных СКЗИ, должен быть рационально минимизирован с тем, чтобы исключить возможность накопления компрометированных ключей

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			ключа должен рассматриваться как фактор противодействия инфраструктурным атакам 4.1.4.18, 4.1.4.19 с тем, чтобы сделать невозможным для потенциального нарушителя накопление в течение длительного срока значительной по масштабам бот-сети из компрометированных теми или иными способами устройств	нарушителем, планирующим массированную атаку на парк УСПД и ПУ, снабженных СКЗИ. Рекомендуемый номинальный срок жизни криптографических ключей, применяемых для защиты УСПД и ПУ, снабженных СКЗИ, составляет 3 месяца
П17	Требование обязательной защиты всех команд управления энергопотреблением при передаче по каналам связи с ИВК	ОТ	В соответствии с требованиями [2] для ПУ, поддерживающих функции управления энергопотреблением, канал передачи команд, связанных с управлением энергопотреблением, должен быть защищен	Передача команд управления энергопотреблением должна осуществляться по сетям общего пользования с применением функции шифрования данных
П18	Требование аутентификации ИВК, как источника данных, для всех команд управления энергопотреблением	ОТ	Для команд управления энергопотреблением кроме защиты канала передачи команд (П17) должна применяться электронная подпись команд управления энергопотреблением со стороны ИВК. Всякая команда управления энергопотреблением должна исполняться на приборе учета только в случае успешной проверки электронной подписи ИВК. Рекомендуется выполнять проверку подписи ИВК на командах управления энергопотреблением на устройстве (приборе), аппаратно	Применение данного требования безопасности исключает возможность несанкционированного управления энергопотреблением даже в случае компрометации криптографических ключей, обеспечивающих защиту канала передачи команд. Закрытый криптографический ключ электронной подписи ИВК должен храниться в единственном экземпляре в режиме, исключающем экспорт данного ключа из устройства хранения, в серверных СКЗИ ИВК в

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			интегрированном с реле управления нагрузкой потребителя	контролируемой зоне центра обработки данных (ЦОД) ИВК. Ключ проверки подписи должен вводиться в устройство в процессе его ввода в эксплуатацию при помощи АРМ управления энергопотреблением должна быть строго адресной и защищена в том числе от повтора
П19	Требования к техническим средствам и технологическому процессу производства ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Технические средства и технологический процесс производства СКЗИ, ПУ и УСПД со встроенными СКЗИ должны быть обеспечены средствами криптографической защиты информации, сертифицированными ФСБ России	Сведения о мерах безопасности технологического процесса производства СКЗИ являются предметом оценки влияния устройства на СКЗИ (П36). СКЗИ, встраиваемые в средства производства ПУ и УСПД, должны быть устойчивы к атакам со стороны пользователя СКЗИ. Процесс производства должен завершаться мероприятиями <ul style="list-style-type: none"> - поэкземплярного учета защищенных продуктов на основе уникальных заводских номеров; - поэкземплярного учета СКЗИ в соответствии с требованиями ФСБ России; контролем целостности среды функционирования СКЗИ, ПО СКЗИ, некриптографических секретов, устанавливаемых на производстве (при наличии), криптографических ключей,

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
				устанавливаемых на производстве (при наличии); - активизацией применяемых мер физической безопасности устройства
П20	Требование отсутствия в составе исправных ПУ, УСПД, СКЗИ ПУ и УСПД криптографических ключей на всех этапах жизненного цикла за исключением этапа эксплуатации	ОТ	В составе ПУ, УСПД, СКЗИ ПУ и УСПД, выпускаемых на производстве, должны отсутствовать криптографические ключи, применяемые на этапе эксплуатации. Такие ключи должны формироваться в составе устройства или вводиться в устройство на этапе ввода устройства в эксплуатацию	Для снижения рисков продукции на этапе передачи в составе ПУ и УСПД рекомендуется применение только некриптографических секретов, без записи криптографических ключей в ПУ и УСПД
П21	Требования к упаковке и транспортировке ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Производство продукции должно завершаться ее упаковкой, позволяющей установить факт вскрытия упаковки при транспортировке и передаче продукции	Рекомендуется указывать на внешней стороне упаковки заводской номер продукции без указания регистрационного (серийного) номера встроенного СКЗИ. Сведения о серийном номере СКЗИ для учета должны передаваться: <ul style="list-style-type: none"> - внутри упаковки продукции; - в энергонезависимой (при наличии технической возможности) памяти с однократной записью или в защищенной памяти устройств
П22	Требования к средствам и технологическому процессу ввода в эксплуатацию ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Технические средства и технологический процесс ввода в эксплуатацию СКЗИ, ПУ и УСПД со встроенными СКЗИ, должны быть обеспечены средствами	Выполнение перечисленных операций ввода ПУ, УСПД, СКЗИ ПУ и УСПД в эксплуатацию должно выполняться, по мере

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>криптографической защиты информации, сертифицированными ФСБ России.</p> <p>На этапе ввода в эксплуатацию должны выполняться следующие мероприятия:</p> <ul style="list-style-type: none"> - проверка заводских номеров устройств и регистрационных номеров СКЗИ; - самодиагностика устройств; допускается также применение внешних средств диагностики; контроль целостности ПО устройств и СКЗИ в составе устройств; - проверка подлинности устройств на основе криптографических механизмов или некриптографических (транспортных) секретов; - подключение, проверка функционирования устройств и тест связи с ИВК; - конфигурирование, настройка устройства; - создание и (или) ввод в состав устройства криптографических ключей и ключевых документов; - проверка защищенного взаимодействия с ИВК; 	<p>возможности, в автоматическом режиме.</p> <p>СКЗИ, встраиваемые в средства ввода в эксплуатацию ПУ и УСПД, должны быть устойчивы к атакам со стороны пользователя СКЗИ, выполняющего ввод УСПД и ПУ, снабженных СКЗИ, в эксплуатацию. В случае выявления неисправностей и (или) нарушений технологического процесса ввода ПУ, УСПД, СКЗИ ПУ и УСПД в эксплуатацию устройство должно сниматься с эксплуатации, криптографические ключи в составе устройства должны быть уничтожены путем вскрытия клеммной коробки, инициированием датчика вскрытия корпуса или иным способом нарушения физической защиты устройства, после чего устройство должно быть передано в ремонт (см. ПЗ1)</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - активизация всех средств физической безопасности устройства; - регистрация всех событий ввода устройства в эксплуатацию в локальном событийном журнале; - передача всех сведений о всех событиях ввода устройства в эксплуатацию в подсистему регистрации сервера ИСУЭ, обеспечивающего ввод приборов в эксплуатацию; - передача в ИВК уведомления об успешном вводе устройства в эксплуатацию; - опломбирование устройства 	
П23	Требования к техническим средствам и технологическому процессу эксплуатации ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	<p>В процессе эксплуатации должны выполняться следующие требования и мероприятия:</p> <ul style="list-style-type: none"> - контроль состояния информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД (см. П2, П4, П24, П33, П37, А15, А16); - управление энергопотреблением с использованием правил П17, П18 и мер защиты А9-А12; - регистрация событий эксплуатации и информационной безопасности в соответствии с требованиями П5-П7 П23, П28; 	<p>Выявленные нарушения правил эксплуатации ПУ, УСПД, СКЗИ ПУ и УСПД должны сопровождаться:</p> <ul style="list-style-type: none"> - уничтожением криптографических ключей в составе устройства путем вскрытия клеммной коробки, инициированием датчика вскрытия корпуса или иным способом нарушения физической защиты устройства (см. П33); - передачей устройства в ремонт (см. П31);

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>реагирование на события эксплуатации и информационной безопасности в соответствии с требованиями (П14, П26, П27, П31, П33, Р1-Р3).</p> <p>В процессе эксплуатации запрещается:</p> <ul style="list-style-type: none"> - управление СКЗИ при помощи средств локального конфигурирования ПУ и УСПД (управление СКЗИ должно осуществляться только централизованно со специализированного сервера в составе ИСУЭ); при этом допускается управление настройками устройства, не влияющими на состояние СКЗИ, при помощи средств локального конфигурирования ПУ и УСПД путем перевода СКЗИ устройства в сервисный режим (см. П30); - подача команд управления энергопотреблением из иных, кроме ИВК, источников; - подача команд управления энергопотреблением от одного прибора учета к другому прибору учета [2] 	<p>повторением штатной процедуры ввода в эксплуатацию (см. П22) после ремонта</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П24	Требования к комплексу организационно-технических мер контроля за состоянием информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД в процессе эксплуатации	ОТ	<p>Контроль за состоянием информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД осуществляется методами:</p> <ul style="list-style-type: none"> - самодиагностики ПУ и УСПД, включая диагностику средств физической защиты ПУ и УСПД (см. П5-П7, П27); - централизованного сбора данных событийного протоколирования, мониторинга и аудита событийных журналов ПУ и УСПД со стороны ИВК; - анализа корректности взаимодействий между ИВК и ПУ (УСПД); - сведением энергобалансов различного уровня, выявление утечек электроэнергии и аномалий в показаниях приборов учета. <p>ПУ и УСПД должны обеспечивать меры безопасности систем событийного протоколирования и аудита П34</p>	<p>В соответствии с требованиями [2] в состав параметров контроля должны входить (не ограничиваясь):</p> <ul style="list-style-type: none"> - дата и время вскрытия клеммной крышки; - дата и время вскрытия корпуса прибора учета; - дата, время, причина включения и отключения встроенного коммутационного аппарата; - дата и время последнего перепрограммирования (в т.ч. дистанционного обновления ПО); - дата, время, тип и параметры выполненной команды; - попытка доступа с неуспешной идентификацией и (или) аутентификацией; - попытка доступа с нарушением правил управления доступом; - попытка несанкционированного нарушения целостности программного обеспечения и параметров; - изменение направления перетока мощности; - дата и время воздействия постоянного или переменного магнитного поля;

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
				<ul style="list-style-type: none"> - факт связи с прибором учета электрической энергии, приведшей к изменению параметров конфигурации, режимов функционирования (в том числе ограничения (возобновления) режима потребления электрической энергии); - дата и время отклонения напряжения в измерительных цепях от заданных пределов; - отсутствие или низкое напряжение при наличии тока в измерительных цепях; - отсутствие напряжения либо значение напряжения ниже запрограммированного; - инверсия фазы или нарушение чередования фаз (для трехфазных приборов учета электрической энергии); - превышение соотношения величин потребления активной и реактивной мощности; - небаланс тока в нулевом и фазном проводе (для однофазных приборов учета электрической энергии); - превышение заданного предела мощности

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П25	Требования к регламенту безопасности эксплуатации ПУ, УСПД, СКЗИ ПУ и УСПД	О	Регламент безопасности эксплуатации ПУ, УСПД, СКЗИ ПУ и УСПД должен быть явно представлен в составе нормативных актов, регулирующих работу ИСУЭ, и должен предусматривать: - выполнение правил безопасности П23, П24, П29, П30; применение мер реагирования на тревожные события (П33), в частности - регламентировать сроки и порядок выездного технического обслуживания ПУ и УСПД, целостность которых была нарушена, вывод из эксплуатации и направление таких ПУ и УСПД на ремонтную процедуру, выполняемую в соответствии с правилами П31	
П26	Требования к процедуре загрузки СФК ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Загрузка СФК ПУ и УСПД должна выполняться после процедуры самодиагностики аппаратной платформы и должна сопровождаться: - проверкой целостности загружаемых данных; - контролем электронной подписи производителя ПУ (УСПД) файлов, содержащих СКЗИ компоненты СФК, прошедшие оценку влияния.	Во избежание сбоев и ошибок при контроле целостности СФК ПУ и УСПД допускаются повторные исполнения контрольных процедур

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>Загрузка устройства, проверка целостности СФК которого дала отрицательный результат, должна экстренно завершаться после выполнения процедур:</p> <p>формирования записи в событийные журналы ПУ (УСПД) и СУЗИ ПУ (УСПД);</p> <ul style="list-style-type: none"> - передачи в ИВК уведомления о нарушении целостности СФК ПУ (УСПД) - в случае, если техническое состояние устройства позволяет осуществить передачу данных в ИВК; - уничтожения криптографических ключей. <p>Устройство, не прошедшее контроль целостности СФК, должно направляться на ремонтную процедуру, выполняемую в соответствии с правилами ПЗ1</p>	
П27	Требования к процедуре диагностики и контроля целостности СФК ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	<p>Диагностика, самодиагностика и контроль целостности СФК ПУ, УСПД, СКЗИ ПУ и УСПД в устройствах, работающих в цикле непрерывной эксплуатации, должны периодически, по запросам ИВК или по таймеру, ПУ - не реже одного раза в 168 часов, УСПД - не реже одного раза в 24 часа, выполнять процедуры самодиагностики и</p>	Во избежание сбоев и ошибок при контроле целостности СФК ПУ и УСПД допускаются повторные исполнения контрольных процедур

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>контроля целостности СФК ПУ, УСПД, СКЗИ ПУ и УСПД.</p> <p>В случае, если проверка целостности СФК ПУ или УСПД дала отрицательный результат, эксплуатация устройства должна экстренно завершаться после выполнения процедур:</p> <ul style="list-style-type: none"> - формирования записи в событийные журналы ПУ (УСПД) и СКЗИ ПУ (УСПД); - передачи в ИВК уведомления о нарушении целостности СФК ПУ (УСПД) - в случае, если техническое состояние устройства позволяет осуществить передачу данных в ИВК; - уничтожения криптографических ключей. <p>Устройство, не прошедшее контроль целостности СФК, должно направляться на ремонтную процедуру, выполняемую в соответствии с правилами ПЗ1</p>	
П28	Требования к процедуре обновления ПО ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	<p>Все обновления программного обеспечения ПУ и УСПД должны проходить оценку влияния (ПЗ6). Процедура обновления программного обеспечения ПУ и УСПД должна выполняться при помощи доверенного сервера в</p>	<p>Обновления, не прошедшие контроля целостности и аутентификации, не должны загружаться в ПУ и УСПД. Рекомендуется выполнять обновления в режиме автоматического восстановления</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>составе ИСУЭ. В процессе обновления программного обеспечения должны выполняться аутентификация источника данных, контроль целостности обновлений и проверка электронной подписи обновления. Загрузка программного обеспечения должна выполняться только в случае положительного результата проверки аутентичности и целостности обновления, а также работоспособности вновь загруженного обновления ПО. При отрицательном результате обновления должны выполняться следующие действия:</p> <ul style="list-style-type: none"> - формирование записи в регистрационном журнале; - передача уведомления в ИВК или на доверенный сервер ИСУЭ, с которого поступило обновление; - уничтожение (удаление из памяти устройства) кода и данных, поступивших в составе обновления. <p>Процесс обновления программного обеспечения ПУ и УСПД должен выполняться автоматически, дистанционно и асинхронно по отношению к процессу обновления ключей и ключевых документов</p>	<p>предыдущей версии ПО в случае аварийного завершения операции обновления</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
П29	Требования по управлению СКЗИ ПУ и УСПД	ОТ	Управление СКЗИ ПУ и УСПД должно выполняться дистанционно из доверенного сервера в составе ИСУЭ только по защищенному каналу. Канал управления ПУ и УСПД должен быть защищен: - механизмами взаимной аутентификации сервера управления и управляемого источника; механизмами обеспечения целостности и конфиденциальности	
П30	Требования по применению средств локального конфигурирования ПУ, УСПД	ОТ	Средства локального конфигурирования ПУ и УСПД могут применяться для чтения, отображения, редактирования, записи текущих настроек ПУ и УСПД уполномоченным для ввода в эксплуатацию УСПД и ПУ, снабженных СКЗИ, сотрудником - до этапа создания и (или) ввода в состав устройства криптографических ключей и ключевых документов (см. П22) или - после (в течение) перевода устройства в сервисный режим. Запрещается применение средств локального конфигурирования ПУ и УСПД, снабженных СКЗИ, для: - управления энергопотреблением;	Сервисный режим УСПД и ПУ, снабженных СКЗИ, предусматривается для выполнения операций локального конфигурирования некриптографических функций устройств и их технического обслуживания (коммутации цепей электрического питания и измерения устройств, замена SIM-карт и т.п.). В сервисном режиме должны выполняться: - отключение датчиков вскрытия клеммной коробки устройства; - опционально - применение дополнительных мер защиты СКЗИ, криптографических ключей и ключевых документов.

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>- управления СКЗИ. Включение сервисного режима должно выполняться при помощи защищенной команды, подаваемой с ИВК или формируемой при помощи СКЗИ, предназначенного для ввода УСПД и ПУ, снабженных СКЗИ, в эксплуатацию.</p> <p>Команда на включение сервисного режима должна приниматься и обрабатываться СКЗИ УСПД и ПУ. События управления УСПД и ПУ, снабженных СКЗИ, при помощи средств локального конфигурирования должны протоколироваться в:</p> <ul style="list-style-type: none"> - событийных журналах управляющего и управляемого устройств; - событийных журналах СКЗИ управляющего и управляемого устройств (включение и выключение сервисного режима). <p>Сведения о событиях локального управления из событийных журналов управляющего и управляемого устройств должны передаваться в ИВК ИСУЭ</p>	В сервисном режиме запрещено отключение датчиков вскрытия корпуса устройства. Функции безопасного применения средств локального конфигурирования должны проверяться при оценке влияния УСПД и ПУ на СКЗИ (П36)
П31	Требования к регламенту технического обслуживания и ремонта ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Техническое обслуживание и ремонт ПУ и УСПД должны осуществляться исключительно в сервисных центрах,	ПУ и УСПД, выпущенные из процедуры ремонта, должны быть по состоянию устройства и его

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>авторизованных на предоставление услуг изготовителями ПУ и УСПД и разработчиком СКЗИ. Процедура технического обслуживания (ремонта) ПУ и УСПД должна включать:</p> <ul style="list-style-type: none"> - уничтожение криптографических ключей в ПУ (УСПД) путем вынужденного срабатывания датчика физической защиты устройства (если ключи не были уничтожены при выводе устройства из эксплуатации; если техническое состояние устройства обеспечивает возможность выполнения операции); - техобслуживание, ремонт; - прошивка программного обеспечения при помощи процедуры, аналогичной принятым на производстве ПУ и УСПД (П19, П20); - тестирование отремонтированных ПУ и УСПД; - при наличии требований - метрологическую поверку ПУ и УСПД; - упаковку ПУ и УСПД в соответствии с требованиями П21 	упаковке аналогичны продукции, выпускаемой с производства. ПУ и УСПД, выпущенные из процедуры ремонта, подлежат вводу в эксплуатацию в соответствии с требованиями П22
П32	Требования к процедуре утилизации ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Перед утилизацией ПУ и УСПД должна выполняться процедура уничтожения криптографических	Критерием успешного выполнения процедуры уничтожения

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			ключей в ПУ (УСПД) путем вынужденного срабатывания датчика физической защиты устройства. После успешного выполнения процедуры уничтожения криптографических ключей ПУ и УСПД дополнительные требования по утилизации ПУ и УСПД не устанавливаются. В случае, если процедура уничтожения криптографических ключей ПУ и УСПД не была выполнена успешно, ПУ и УСПД должны передаваться для утилизации изготовителю	криптографических ключей в ПУ (УСПД) является вывод сообщения об отсутствии криптографических ключей в ПУ (УСПД) или передача соответствующего сообщения на устройство локального конфигурирования (удаленный дисплей)
П33	Требования к процедурам мониторинга, сигнализации ПУ, УСПД, СКЗИ ПУ и УСПД в тревожных ситуациях	ОТ	<p>Все события контроля, перечисленные в требованиях П5, должны выступать в качестве минимального набора событий (параметров) мониторинга состояния ПУ, УСПД, СКЗИ ПУ и УСПД. Для всех событий, представляющих собой отклонения от норм, установленных оператором ИСУЭ, должны:</p> <ul style="list-style-type: none"> - формироваться записи в событийные журналы ПУ, УСПД, СКЗИ ПУ и УСПД; - осуществляться передача сведений о событиях в ИВК ИСУЭ. 	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>ПУ и УСПД должны в инициативном порядке формировать и передавать в ИВК сообщения тревожной сигнализации при возникновении событий из списка:</p> <ul style="list-style-type: none"> - срабатывания датчика внешних полей; - срабатывания внешнего датчика вскрытия (или иного датчика проникновения) монтажного шкафа, в котором расположено УСПД; - нарушения параметров электроснабжения; - выявления фактов изменения (искажения) информации (за исключением нарушений целостности СФК); - приема команды ИВК на управление энергопотреблением, без применение электронной подписи ИВК, приема команды ИВК на управление энергопотреблением с нарушением электронной подписи или повторного приема одной и той же команды ИВК на управление энергопотреблением; - приема команды управления СКЗИ ПУ и УСПД по открытому каналу передачи данных, приема управления СКЗИ с нарушением электронной подписи или повторного 	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>приема одной и той же команды управления СКЗИ;</p> <ul style="list-style-type: none"> - обнаружения признаков попыток несанкционированного доступа по коммуникационным каналам (получение нецелостных сообщений, многократные неудачные попытки аутентификации и т.п.). <p>ПУ и УСПД должны выполнять функции формирования сообщений тревожной сигнализации и уничтожения криптографических ключей в соответствии с требованиями П11-П14 при возникновении событий из списка:</p> <ul style="list-style-type: none"> - срабатывания датчика вскрытия корпуса ПУ и УСПД; - срабатывания датчика вскрытия клеммной коробки ПУ или блока коммутации (коммутационного аппарата) УСПД; - нарушения целостности СКЗИ и (или) СФК СКЗИ ПУ и УСПД. <p>ИВК должен обеспечивать:</p> <ul style="list-style-type: none"> - периодический контроль версий прошивок ПУ и УСПД и сравнение со списком актуальных прошивок; - периодический контроль ухода времени на ПУ и УСПД более 	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>задаваемого оператором ИВК предела;</p> <ul style="list-style-type: none"> - возможность ведения оператором списка ПУ и УСПД, которые должны содержать СКЗИ, и сигнализацию оператору о невозможности связи с ПУ и/или УСПД по криптографически защищенному каналу 	
П34	Требования к механизмам событийного протоколирования	ОТ	<p>ПУ и УСПД должны обеспечивать:</p> <ul style="list-style-type: none"> - энергонезависимое хранение журнала событий; - инкрементальный счетчик событий; - выявление фактов изменения (искажения) информации, хранящейся в журналах событий; выявление фактов изменения (искажения) программного обеспечения ПУ и УСПД, включая средства событийного протоколирования. <p>СКЗИ ПУ и УСПД должны обеспечивать ведение в энергонезависимой памяти отдельного событийного журнала, в который вносятся:</p> <ul style="list-style-type: none"> - события жизненного цикла СКЗИ, такие, как ввод в эксплуатацию, смена криптографических ключей, 	Требования к механизмам событийного протоколирования должны контролироваться при оценке влияния УСПД на СКЗИ (П36)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>включение и выключение сервисного режима и т.п.;</p> <ul style="list-style-type: none"> - события информационной безопасности СКЗИ, включая подозрительные события (состав событий данного типа уточняется при проектировании СКЗИ). <p>Событийный журнал СКЗИ должен быть снабжен:</p> <ul style="list-style-type: none"> - сведениями о дате и времени регистрируемых событий; - инкрементальным счетчиком событий; - цепью связанных хэш-сумм, рассчитываемых с учетом данных текущего события и всей предыстории, записанной в журнал событийного протоколирования. <p>При передаче в ИВК сведения из событийного журнала СКЗИ должны быть защищены электронной подписью ПУ или УСПД, при приеме этих сведений в ИВК должна выполняться проверка электронной подписи источника данных</p>	
П35	Применение принципов безопасного дизайна встроенных программных систем	Т	При проектировании, конфигурировании и настройке программного обеспечения ПУ и УСПД должны соблюдаться следующие принципы разработки	Аспекты безопасного дизайна программного обеспечения ПУ и УСПД должны быть включены в состав анализа исходных кодов программного обеспечения при

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>безопасного программного обеспечения встроенных систем:</p> <ul style="list-style-type: none"> - должны использоваться безопасные языки программирования и средства разработки; программные библиотеки, используемые при разработке ПО, не должны вносить избыточности и недеklarированных возможностей; особое внимание должно быть уделено безопасной загрузке кода СФК, включающей проверку электронной подписи загружаемого кода, контроль источника и адресов загрузки ПО; - должны быть предусмотрены меры по обеспечению безопасности процессов управления памятью, защите областей, в которых хранятся критические данные, имеющимися аппаратными средствами защиты П8, очистке при освобождении памяти, в которой хранились критические данные; - должны применяться разделы для хранения кода и данных встроенной системы; должен осуществляться контроль доступа к разделам, в которых размещаются код и данные СКЗИ со стороны всех прочих разделов; 	<p>выполнении процедур оценки влияния ПУ и УСПД на СКЗИ (П36)</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - для сетевых соединений должны выполняться требования: - минимизации количества открытых портов (соединений); - сетевого контроля доступа; - применения передачи по каналам связи криптографически защищенных данных во всех случаях, кроме тех, где нельзя избежать обменов открытыми данными; - изоляция принимаемых из сети и передаваемых в сеть данных, исключение ситуаций в которых управление процессора передается на адреса, содержащиеся в принимаемых или передаваемых данных (за исключением процедур обновления программного обеспечения, выполненных с соблюдением требований П28). - в случае выявления уязвимостей в процессе разработки и эксплуатации должно в приоритетном порядке разрабатываться обновление, устраняющее уязвимость; обновления ПО подлежат оценке влияния (П36) 	
П36	Анализ СФК СКЗИ ПУ и УСПД в процессе оценки влияния	ОТ	Проверка требований к ПУ, УСПД, СКЗИ ПУ и УСПД П5-П7, П11-П14, П19, П26, П27, П30, П34, П35 должна выполняться в процессе	Методика оценки влияния должна быть согласована ФСБ России

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			оценки влияния ПУ (УСПД) на встроенные СКЗИ	
П37	Нормативно-правовая база эксплуатации ПУ, УСПД, СКЗИ ПУ и УСПД	О	Администрацией ИСУЭ должен быть разработан и введен в действие комплекс нормативно-правовых документов, включающий методические рекомендации, технологические инструкции и регламенты, обеспечивающих выполнение требований к проактивным мерам информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД	
АКТИВНЫЕ МЕРЫ ЗАЩИТЫ				
A1	Защищенный процесс производства ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	Технологический процесс производства ПУ, УСПД, СКЗИ ПУ и УСПД должен осуществляться с выполнением требований П19-П21	Производство ПУ и УСПД со встроенными СКЗИ должен выполнять лицензиат ФСБ России с применением средств криптографической защиты, сертифицированных ФСБ России
A2	Контроль целостности упаковки при передаче и перед монтажом ПУ, УСПД, СКЗИ ПУ и УСПД	ОТ	При передаче ПУ и УСПД должна контролироваться целостность заводской упаковки продукции или упаковки, сформированной в сервисном центре с выполнением требований П21	Продукция, передаваемая в упаковке с нарушениями целостности, должна быть распакована, проведена через процедуру уничтожения ключей П14, Р1 и передана в ремонт (П31, Р2)
A3	Защищенный процесс ввода в эксплуатацию (регистрации) ПУ и УСПД	ОТ	Процесс ввода в эксплуатацию ПУ и УСПД должен выполняться с исполнением мер защиты, включающих:	Процесс ввода в эксплуатацию ПУ и УСПД должен выполняться уполномоченным администрацией ИСУЭ сотрудником в

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - контроль одобрения типа продукции, допуска к эксплуатации; - контроль целостности упаковки П21, А2; - контроль средств идентификации ПУ и УСПД, проверку сведений об устройстве в соответствии с требованиями П22; - проверку подлинности устройства (А4); - опционально - настройку устройства с применением средств локального конфигурирования УСПД и ПУ, снабженных СКЗИ, с соблюдением требований П30; - персонализацию СКЗИ (А5); - проверку подключения к ИВК; - инициализацию средств физической (А6) и логической (А7, А8) защиты 	<p>полуавтоматическом режиме с использованием специализированного автоматизированного рабочего места (АРМ) регистрации, снабженного СКЗИ, сертифицированным ФСБ России. Факт невозможности ввода ПУ и УСПД в эксплуатацию без применения АРМ регистрации должен проверяться на этапе оценки влияния ПУ и УСПД на встроенные СКЗИ (П36)</p>
А4	Проверка транспортных секретов перед вводом в эксплуатацию	Т	<p>Для ПУ и УСПД, вводимых в эксплуатацию, должны проверяться транспортные (некриптографические) секреты, записанные на производстве или в сервисном центре. Значение секрета должно:</p> <ul style="list-style-type: none"> - соответствовать значению, записанному в доверенный сервер ИСУЭ при производстве ПУ (УСПД); 	<p>ПУ и УСПД, для которых обнаружено несоответствие транспортного секрета, должны быть проведены через процедуру уничтожения ключей П14, Р1 и переданы в ремонт (П31, Р2)</p>

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			быть уникальным (не должно повторяться)	
A5	Персонализация СКЗИ при вводе в эксплуатацию	ОТ	Персонализация СКЗИ должна выполняться при вводе ПУ, УСПД, СКЗИ ПУ и УСПД в эксплуатацию после успешного выполнения меры безопасности А3. Персонализация СКЗИ должна включать операции: <ul style="list-style-type: none"> - доверенной загрузки ключевых документов (корневых сертификатов) доверенного сервера ИСУЭ; - создания криптографических ключей и ключевых документов; - регистрации сведений о вводимом в эксплуатацию устройстве в ИВК (доверенном сервере ИСУЭ); - проверки работоспособности защищенного взаимодействия с ИВК (доверенным сервером ИСУЭ) 	Персонализация СКЗИ должна выполняться лицензиатом ФСБ России при помощи АРМ регистрации, сертифицированного ФСБ России. ПУ и УСПД, для которых при вводе в эксплуатацию возникли (обнаружены) неустраняемые ошибки, должны быть проведены через процедуру уничтожения ключей П14, Р1 и переданы в ремонт (П31, Р2)
A6	Применение мер физической безопасности ПУ и УСПД	Т	Для ПУ и УСПД должны применяться меры физической защиты контролируемой зоны внутри корпуса устройства П5. Средства защиты и контроля должны быть активированы при вводе устройства в эксплуатацию и работать в непрерывном режиме вплоть до вывода устройства из эксплуатации (за исключением операций перевода УСПД и ПУ,	При нарушении мер физической безопасности ПУ и УСПД должны выполняться требования П11-П14 и применяться меры Р1-Р3. Для ПУ и УСПД наличие мер физической безопасности П5-П7 и выполнение требований П11- П14 должны контролироваться на этапе оценки влияния ПУ и УСПД на СКЗИ (П36)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			снабженных СКЗИ, в сервисный режим, см. П30)	
A7	Применение мер защиты СФК ПУ	T	<p>Приборы учета, имеющие встроенные СКЗИ, в процессе эксплуатации, наряду с общими требованиями П23, должны выполнять следующие меры защиты СФК:</p> <ul style="list-style-type: none"> - меры физической защиты контролируемой зоны внутри прибора А6 в соответствии с требованиями П5, П6, П11, П12, П30; - хранение криптографических ключей и критических данных в защищенной памяти с использованием механизмов П8 (при наличии технической возможности); - защищенный процесс загрузки ПО СФК и обновления ПО СФК (П26- П28); - процедуры диагностики и самодиагностики (П24, П27); - меры защиты данных и сетевой безопасности А9, А12 в соответствии с требованиями П2, П17, П18; - меры безопасности процессов управления ПУ в соответствии с требованиями П10, П29, П30, включая меры защиты управления энергопотреблением П17, П18; 	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - меры внутреннего (П24) и внешнего (П33, А16) мониторинга информационной безопасности ПУ; - меры реагирования на подозрительные события и инциденты информационной безопасности (Р1-Р3) 	
А8	Применение мер защиты СФК УСПД	Т	<p>Устройства сбора и передачи данных в процессе эксплуатации, наряду с общими требованиями П23, должны выполнять следующие меры защиты СФК:</p> <ul style="list-style-type: none"> - меры физической защиты контролируемой зоны внутри УСПД А6 в соответствии с требованиями П7, П13; - хранение криптографических ключей и критических данных в защищенной памяти с использованием механизмов П9 (при наличии технической возможности); - защищенный процесс загрузки ПО СФК и обновления ПО СФК (П26- П28); процедуры диагностики и самодиагностики (П24, П27); - меры защиты данных и сетевой безопасности А10, А12 в соответствии с требованиями П2, П17, П18; 	В процессе эксплуатации УСПД должны применяться меры защиты ОС УСПД в соответствии с требованием П7

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - меры безопасности процессов управления УСПД в соответствии с требованиями П10, П29, П30, включая меры защиты управления энергопотреблением П17, П18; - меры внутреннего (П24) и внешнего (П33, А16) мониторинга информационной безопасности УСПД; - меры реагирования на подозрительные события и инциденты информационной безопасности (Р1-Р3) 	
А9	Применение мер сетевой безопасности ПУ	Т	<p>Для ПУ в процессе эксплуатации должны выполняться требования сетевой информационной безопасности, содержащиеся в требованиях П2, П6, П10, П17, П18, П29.</p> <p>Для ПУ, работающих без операционной системы, при прямом подключении к ИВК наиболее действенными мерами защиты являются:</p> <ul style="list-style-type: none"> - минимизация сетевых взаимодействий, соединений, устанавливаемых ПУ; ограничение сетевых портов, прослушивающих вызовы со стороны ИВК; 	При эксплуатации ПУ рекомендуется включать механизмы тотальной защиты трафика приборов учета при взаимодействии с ИВК и доверенными серверами ИСУЭ и полностью исключать обмена открытой информацией (см. П5)

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<ul style="list-style-type: none"> - отсутствие открытых соединений, если ПУ не находится в режиме приема/передачи данных; - сетевой контроль доступа; - аутентификация источника данных и шифрование данных при взаимодействии с ИВК; - разделение ресурсов (формирование разделов) программного обеспечения ПУ, исключение передачи управления по адресам, на которых хранятся принимаемые/передаваемые данные и другие принципы безопасного дизайна программного обеспечения (ПЗ5) 	
A10	Применение мер сетевой безопасности УСПД	Т	Для УСПД, работающих без операционной системы, должен выполняться комплекс мер А9. Для УСПД, работающих на основе операционной системы, дополнительно должен применяться комплекс мер сетевой безопасности, присущих для конкретного типа ОС УСПД, включенный в оценку влияния в соответствии с требованиями П7	При эксплуатации УСПД рекомендуется включать механизмы тотальной защиты трафика приборов учета при взаимодействии с ИВК и доверенными серверами ИСУЭ и полностью исключать обмена открытой информацией (см. П5). В процессе эксплуатации УСПД должны применяться меры сетевой безопасности, присущие ОС УСПД в соответствии с требованием П7
A11	Обновление криптографических ключей	Т	Криптографические ключи, применяемые для взаимной аутентификации объектов и для	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			защиты информационных обменов по открытым сетям передачи данных должны обновляться по безопасному протоколу, соответствующему требованиям ФСБ России (П3). Протокол обновления ключей должен обеспечивать автономную работу ПУ и УСПД в течение назначенного срока автономной эксплуатации (П15)	
A12	Защищенный процесс дистанционного управления со стороны ИВК	Т	<p>Все информационные обмены, связанные с управлением ПУ и УСПД, должны быть защищены (П2, П17, П29) при помощи:</p> <ul style="list-style-type: none"> - взаимной аутентификации объектов взаимодействия; - шифрования. <p>Команды, связанные с управлением энергопотреблением, должны быть дополнительно защищены при помощи электронной подписи ИВК (П18). Состав команд, связанных с управлением энергопотреблением, может зависеть от особенностей реализации конкретной модели ИВК и должен уточняться в процесса разработки проекта ИСУЭ в защищенном исполнении</p>	
A13	Меры безопасности процесса управления при помощи средств локального конфигурирования	Т	Средства локального конфигурирования ПУ и УСПД должны применяться исключительно	Управление энергопотреблением и управление СКЗИ при помощи средств локального

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			сервисном режиме эксплуатации УСПД и ПУ, снабженных СКЗИ, с исполнением требований П23 и П30	конфигурирования должно быть запрещено. Применение средств локального управления должно ограничиваться настройками конфигурации УСПД или ПУ, не влияющими на состояние и функционирование СКЗИ
A14	Контроль и диагностика состояния информационной безопасности ПУ	Т	ПУ в процессе эксплуатации должны непрерывно осуществлять контроль состояния средств физической защиты (П5, П6, П11, П12), контроль целостности СФК (П24, П27, П33, П37). Сведения о выявленных событиях и инцидентах безопасности должны регистрироваться в событийных журналах и передаваться в ИВК	При выявлении нарушений требований физической безопасности и целостности СФК ПУ и УСПД должны выполняться требования П11- П14 и применяться меры Р1-Р3
A15	Контроль и диагностика состояния информационной безопасности УСПД	Т	УСПД в процессе эксплуатации должны непрерывно осуществлять контроль состояния средств физической защиты (П7, П13), контроль целостности СФК (П24, П27, П33, П37). Сведения о выявленных событиях и инцидентах безопасности должны регистрироваться в событийных журналах и передаваться в ИВК. Дополнительно УСПД должны вести мониторинг состояния подключения обслуживаемых ими приборов учета, принимать от них сообщения о	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			событиях эксплуатации и информационной безопасности, регистрировать эти события и передавать сведения об этих событиях в ИВК	
A16	Мониторинг безопасности ПУ и УСПД со стороны ИВК	T	<p>В ИСУЭ должен быть организован отдельный процесс мониторинга состояния ПУ, УСПД, СКЗИ ПУ и УСПД, основанный на:</p> <ul style="list-style-type: none"> - событиях эксплуатации и информационной безопасности, сведения о которых поступают от ПУ и УСПД; - событиях и данных целевого функционирования ПУ и УСПД (нормах и аномалиях показателей потребления электроэнергии, поступающих от ПУ и УСПД, энергобалансам объектов и т.п.); сведениях, поступающих от эксплуатирующих организаций объектов энергоснабжения и потребителей электроэнергии 	По результатам мониторинга безопасности ПУ и УСПД в ИВК могут приниматься реактивные меры безопасности Р2, Р3, в случае явного указания на нарушение целостности ПУ или компрометацию СКЗИ ПУ должна применяться мера Р1 и, затем, Р2
РЕАКТИВНЫЕ МЕРЫ ЗАЩИТЫ				
P1	Уничтожение криптографических ключей в случае инцидентов безопасности или обоснованных подозрений о нарушениях	T	В случае нарушения целостности корпуса ПУ или УСПД и (или) явного указания на иное нарушение контролируемой зоны эксплуатации ПУ или УСПД или при получении соответствующей команды от ИВК (П14) СКЗИ ПУ (УСПД) должны	ПУ и УСПД, для которых была выполнена процедура уничтожения криптографических ключей, должны выводиться из эксплуатации и направляться в ремонт (П31, 32). Для ПУ (УСПД), выполнивших операцию

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			<p>выполнять операцию уничтожения криптографических ключей. При выполнении операции уничтожения криптографических ключей должно быть сформировано и передано в ИВК сообщение о событии, послужившем основанием для уничтожения криптографических ключей.</p> <p>После уничтожения ключей ПУ (УСПД) может отвечать на запросы ИВК о показаниях измерений в открытом режиме. Исполнение любых команд управления (перевод в сервисный режим, изменение настроек ПУ и УСПД, управление энергопотреблением, обновление программного обеспечения и т.п.) для ПУ и УСПД с уничтоженными ключами запрещено</p>	уничтожения криптографических ключей, допускается передача в ИВК показаний измерений. При этом в ответ на любой запрос ИВК должно включаться сигнальное сообщение об уничтожении криптографических ключей и невозможности обеспечивать штатное функционирование ПУ (УСПД)
P2	Выездное техническое обслуживание и ремонт ПУ и УСПД, целостность которых была нарушена	ОТ	В случае длительного отсутствия связи с ИВК без признаков нарушения целостности корпуса устройства допускается перевод устройства в сервисный режим в соответствии с требованиями ПЗ0 и проведение диагностики устройства при помощи средств локального конфигурирования, перекоммутации цепей электропитания и линий связи и замены SIM-карты. В случае	

Номер пункта	Наименование меры защиты	Тип	Механизм защиты	Оценка стойкости, зона применения меры защиты
			выявления неисправностей устройства и (или) при выполнении операции уничтожения криптографических ключей (П14) ПУ (УСПД), содержащий СКЗИ, должен сниматься с объекта эксплуатации и передаваться в сервисную организацию изготовителя ПУ (УСПД) для выполнения ремонтных процедур с выполнением требований ПЗ1	
РЗ	Расследование инцидентов информационной безопасности ПУ и УСПД	ОТ	Инциденты информационной безопасности, как минимум те из них, которые привели к выполнению операции уничтожения криптографических ключей, должны быть предметом расследования администрации безопасности ИСУЭ. Результатом такого мероприятия должно быть заключение по результатам расследования инцидента	В случае, если расследуемый инцидент информационной безопасности ПУ (УСПД) мог привести к компрометации СКЗИ, в состав следственных мероприятий должна входить экспертиза разработчика СКЗИ. Заключение экспертизы разработчика СКЗИ должно прилагаться к заключению по результатам расследования инцидента

4.5 ОЦЕНКА ЭФФЕКТИВНОСТИ МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСПД, ПУ И СКЗИ УСПД И ПУ

Оценка эффективности мер противодействия угрозам информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ приведена в таблице 4.

Т а б л и ц а 4

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ ПРОИЗВОДСТВА					
4.1.1.1	Ошибка проектирования	С	Оценка влияния ПЗ6, сертификация СКЗИ ПЗ и комплекс мер контроля состояния ПУ, УСПД, СКЗИ ПУ и УСПД на различных этапах жизненного цикла ПУ и УСПД (ПЗ, П19, П24, П26, П27, П35, А1, А13-А15, Р3)	П	
4.1.1.2	Дефект, брак, недекларированные возможности	С	См. 4.1.1.1	Н	
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ ПЕРЕДАЧИ					
4.1.2.1	Несанкционированный доступ, вскрытие	Н	Общие требования по защите СФК СКЗИ, включая требования физической защиты ПУ и УСПД П5-П7, меры безопасности производства, в т.ч. защищенная упаковка П19, П21, отсутствие в ПУ и УСПД криптографических ключей П20, контроль ПУ и УСПД при вводе в эксплуатацию П22, расследование инцидентов Р3	Н	Непосредственно в процессе передачи ПУ и УСПД основной мерой безопасности является упаковка и контроль ее целостности. Однако атаки на ПУ, УСПД, СКЗИ ПУ и УСПД в процессе передачи с высокой вероятностью будут выявлены на последующих этапах жизненного цикла ПУ и УСПД при помощи перечисленных мер безопасности
4.1.2.2	Несанкционированная модернизация	Н	Наряду с мерами защиты от атаки 4.1.2.1 применяются меры безопасности П8-П9	Н	
4.1.2.3	Подмена, фальсификация	С	Общие требования по защите СФК СКЗИ, включая требования уникальной идентификации ПУ и УСПД П5-П7, меры безопасности производства, в т.ч. защищенная упаковка П19, П21, контроль транспортных секретов ПУ и УСПД при вводе в эксплуатацию П22	П	Подмена, фальсификация ПУ и УСПД на этапе передачи будут выявлены в ходе ввода в эксплуатацию в силу контроля транспортных секретов ПУ и УСПД при помощи сертифицированного ФСБ России как СКЗИ КСЗ АРМ

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					регистрации и сверки их с записями в доверенных серверах ИСУЭ (см. 4.1.3.1)
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ И УСПД НА ЭТАПЕ ВВОДА В ЭКСПЛУАТАЦИЮ					
4.1.3.1	Несанкционированная модернизация	С	Выполнение требований безопасности ввода ПУ и УСПД в эксплуатацию достигается за счет применения комплекса мер безопасности П22, в т.ч. применения АРМ регистрации ПУ и УСПД. Инциденты информационной безопасности на этом этапе подлежат расследованию РЗ	Н	
4.1.3.2	Компрометация криптографических ключей устройства	С	В комплексе защиты от атаки 4.1.3.2 является полный состав мер безопасности, применяемый против атаки 4.1.2.2. Непосредственной мерой защиты криптографических ключей на этапе ввода в эксплуатацию является защищенный процесс персонализации СКЗИ, выполняемый при помощи АРМ регистрации, сертифицированного ФСБ России	П	Основанием для оценки риска, как пренебрежимо малого является полный состав мер защиты АРМ регистрации, контролируемый при сертификации
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ И УСПД НА ЭТАПЕ ЭКСПЛУАТАЦИИ					
4.1.4.1	Несанкционированная модернизация путем физического вмешательства в работу устройства	П	Разработка ПУ и УСПД с учетом требований безопасности П5-П7, использование встроенных функций безопасности платформ П8-П9	П	
4.1.4.2	Компрометация криптографических ключей устройства	С	Выполнение требований безопасности П5-П7, применение сертифицированных СКЗИ для защиты ПУ и УСПД ПЗ, оценка влияния СФК ПЗ6, интеграция средств физической защиты с СКЗИ П11-П13, уничтожение	Н	

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
			криптографических ключей в случае нарушения физической защиты устройства П14, П36, Р1, процесс обновления криптографических ключей П15, А11 и минимизация срока жизни криптографических ключей П16, обеспечение мер безопасности эксплуатации ПУ и УСПД П23- П25, А6-А9, мер сетевой защиты А9, А10, меры контроля безопасности А13-А15, реактивные меры безопасности Р1-Р3		
4.1.4.3	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и УСПД	В	Основной мерой защиты является А10	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме шифрования трафика для всех информационных обменов между ИВК и УСПД. В случае наличия между ИВК и УСПД обменов открытым трафиком атака 4.1.4.3 реализуется со 100%-й вероятностью, в то время как защищенный трафик будет этой атаке практически не подвержен. Оценка остаточного риска «средний» сделана на том основании, что в соответствии со стандартом [10] открытый трафик содержит в себе сведения, компрометация которых наносит малый ущерб ИСУЭ. Вместе с тем открытый трафик может использоваться для разведки конфигурации ИСУЭ, поиска

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					уязвимостей ПУ, УСПД и ИВК, несанкционированного доступа к ПУ, УСПД и ИВК. Рекомендуется режим тотальной защиты трафика УСПД при помощи шифрования
4.1.4.4	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между ИВК и ПУ	В	Основной мерой защиты является А9	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме шифрования трафика для всех информационных обменов между ИВК и ПУ. В случае наличия между ИВК и ПУ обменов открытым трафиком атака 4.1.4.4 реализуется со 100%-й вероятностью, в то время как защищенный трафик будет этой атаке практически не подвержен. Оценка остаточного риска «средний» сделана на том основании, что в соответствии со стандартом [10] открытый трафик содержит в себе сведения, компрометация которых наносит малый ущерб ИСУЭ. Вместе с тем открытый трафик может использоваться для разведки конфигурации ИСУЭ, поиска уязвимостей ПУ, УСПД и ИВК, несанкционированного доступа к ПУ, УСПД и ИВК. Рекомендуется режим тотальной защиты трафика ПУ при помощи шифрования даже

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					при включении ПУ в сеть ИСУЭ при помощи УСПД
4.1.4.5	Перехват информационных обменов, нарушение целостности и конфиденциальности обменов между УСПД и ПУ	С	Комплекс мер физической безопасности ПУ и УСПД (П9, П11-П13), безопасности эксплуатации ПУ и УСПД (П24, П25) и защита коммуникаций между ними (А9б А10)	П	
4.1.4.6	Криптоанализ	С	Мерами защиты от атаки 4.1.4.6 являются: - защита сетевых взаимодействий А9, А10; требование отсутствия в составе исправных ПУ, УСПД, СКЗИ ПУ и УСПД криптографических ключей на всех этапах жизненного цикла ПУ и УСПД, кроме этапа эксплуатации П20; - уничтожение криптографических ключей при подозрительных событиях Р1, при передаче в ремонт П31 и при утилизации П32; - меры защиты криптографических ключей П14-П16	П	Основными мерами безопасности, позволяющими оценить остаточный риск атаки 4.1.4.6, как «пренебрежимо малый», являются требования сертификации СКЗИ ПУ и УСПД П3 и оценки влияния П3б
4.1.4.7	Навязывание ложных партнеров по взаимодействию между ИВК и УСПД	В	Основной мерой защиты является А10	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая применения сертифицированных СКЗИ в режиме шифрования трафика для всех информационных обменов между ИВК и УСПД. В случае наличия между ИВК и УСПД обменов открытым трафиком риск атаки 4.1.4.7 оценивается как «средний» (см. дополнительно 4.1.4.3).

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					Рекомендуется режим тотальной защиты трафика УСПД при помощи шифрования
4.1.4.8	Навязывание ложных партнеров по взаимодействию между ИВК и ПУ	В	Основной мерой защиты является А9	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме шифрования трафика для всех информационных обменов между ИВК и ПУ. В случае наличия между ИВК и ПУ обменов открытым трафиком риск атаки 4.1.4.8 оценивается как «средний» (см. дополнительно 4.1.4.4). Рекомендуется режим тотальной защиты трафика ПУ при помощи шифрования
4.1.4.9	Навязывание ложных партнеров по взаимодействию между УСПД и ПУ	С	Комплекс мер физической безопасности ПУ и УСПД и коммуникаций между ними (А9, А10)	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме тотального шифрования трафика для всех информационных обменов между ИВК и ПУ. В случае наличия между ИВК и ПУ обменов открытым трафиком риск атаки оценивается как «средний»
4.1.4.10	Сетевое вторжение, несанкционированный доступ к ПУ	В	ПУ защищается от несанкционированного доступа из сети путем применения следующих мер защиты: - методы дизайна безопасной архитектуры сетевых взаимодействий (см. ПЗ5); - применением мер сетевой безопасности А9	П (С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме тотального шифрования трафика для всех информационных обменов между ИВК и ПУ. В случае

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					наличия между ИВК и ПУ обменов открытым трафиком риск атаки 4.1.4.10 обеспечивается, преимущественно, методами безопасного дизайна и сетевого контроля доступа. В этом случае риск оценивается как «средний» (см. дополнительно 4.1.4.4). Рекомендуется режим тотальной защиты трафика ПУ при помощи шифрования
4.1.4.11	Сетевое вторжение, несанкционированный доступ к УСПД	В	УСПД защищается от несанкционированного доступа из сети путем применения следующих мер защиты: <ul style="list-style-type: none"> - методы дизайна безопасной архитектуры сетевых взаимодействий (см. П35); - подготовка операционной системы УСПД для снижения уровня уязвимости по отношению к атакам несанкционированного доступа из сети П7; функции операционной системы, включаемые для сетевого контроля доступа и представляемые для оценки влияния П7, П36; - применением мер сетевой безопасности А9 	П (Н или С)	Оценка остаточного риска «пренебрежимо малый» сделана для случая сертифицированных СКЗИ в режиме шифрования трафика для всех информационных обменов между ИВК и УСПД. В случае наличия между ИВК и УСПД обменов открытым трафиком риск атаки 4.1.4.111 обеспечивается, преимущественно, методами безопасного дизайна и сетевого контроля доступа. В этом случае риск оценивается как «средний» или низкий в зависимости от качества присущих операционной системе УСПД средств защиты (см. П7). Рекомендуется режим тотальной защиты трафика УСПД при помощи шифрования

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
4.1.4.12	Внедрение вредоносного программного обеспечения в ПУ	В	Методы защиты аналогичны 4.1.4.10	П (С)	См. 4.1.4.10. Рекомендуется режим тотальной защиты трафика УСПД при помощи шифрования
4.1.4.13	Внедрение вредоносного программного обеспечения в УСПД	В	Методы защиты аналогичны 4.1.4.11 с дополнением функций защиты от вредоносного ПО, присущих ОС УСПД	П (Н или С)	См. 4.1.4.11. Рекомендуется режим тотальной защиты трафика УСПД при помощи шифрования
4.1.4.14	Перехват управления при взаимодействии ИВК и ПУ	В	Взаимная аутентификация, шифрование всех информационных обменов между ИВК и ПУ, связанных с управлением ПУ и управлением энергопотреблением (А9). Меры защиты канала управления энергопотреблением, описанные в требованиях П17, П18	П	При реализации функций защиты информации при помощи сертифицированных ФСБ России средств информационной безопасности риск оценивается как «пренебрежимо малый»
4.1.4.15	Перехват управления при взаимодействии ПУ и УСПД	В	Взаимная аутентификация, шифрование всех информационных обменов между ИВК и УСПД, связанных с управлением ПУ, УСПД и управлением энергопотреблением (А10). Меры защиты канала управления энергопотреблением, описанные в требованиях П17, П18	П (С)	При реализации функций защиты информации при помощи сертифицированных ФСБ России средств информационной безопасности в режиме тотального шифрования трафика риск оценивается как «пренебрежимо малый». В случае наличия между ИВК, УСПД и ПУ обменов открытым трафиком риск оценивается как «средний» (см. обоснование 4.1.4.9)
4.1.4.16	Несанкционированное применение локального конфигуратора ПУ	Н	Выполнение требований к техническим средствам и технологическому процессу эксплуатации ПУ, СКЗИ ПУ (П23, П30, А13)	Н	При использовании средств локального конфигурирования, исключительно в сервисном режиме (см П30) риск оценивается как «низкий»

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
4.1.4.17	Несанкционированное применение локального конфигуратора УСПД	Н	Выполнение требований к техническим средствам и технологическому процессу эксплуатации УСПД, СКЗИ УСПД (П23, А13). Применение СКЗИ на средствах локального конфигурирования УСПД (П30)	Н	См. 4.1.4.16.
4.1.4.18	Атаки на инфраструктуру энергопотребления путем массовой компрометации ПУ и УСПД	В	Меры защиты от атак 4.1.2.2, Смена криптографических ключей (П15), минимизация срока жизни криптографических ключей (П16), не позволяющая даже в случае компрометации единичных устройств накопить в течение длительного времени значительный массив компрометированных ключей для массовой атаки (в силу устаревания компрометированного материала). Защита взаимодействий ИВК с ПУ и УСПД П3, П5-П7, П35, А9, А10, в том числе меры защиты канала управления энергопотреблением П17 и П18	П	Риск оценивается как «пренебрежимо малый» по причинам: - накопление значительной бот-сети из компрометированных ПУ и УСПД крайне маловероятно (см. 4.1.4.1, 4.1.4.2); - взлом зашифрованных каналов управления, защищенных при помощи СКЗИ, сертифицированных ФСБ России, крайне маловероятен (см. 4.1.4.14, 4.1.4.15); - даже в случае маловероятного события успешного выполнения атак 4.1.4.1, 4.1.4.2, 4.1.4.14, 4.1.4.15 применение для защиты команд управления энергопотреблением для ПУ и УСПД электронной подписи ИВК исключает навязывание прибору ложной команды. Поскольку секретный ключ электронной подписи ИВК хранится в доверенных серверах ИСУЭ и не содержится в СКЗИ ПУ и УСПД, нарушитель,

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
					скомпрометировавший ПУ или УСПД, не имеет возможности фальсифицировать подпись ИВК
4.1.4.19	Атаки на инфраструктуру энергопотребления со стороны компрометированного ПУ или УСПД	В	Защита взаимодействий ИВК с ПУ и УСПД ПЗ, П5-П7, П35, А9, А10, в том числе меры защиты канала управления энергопотреблением П17 и П18	Н	Риск оценивается как «низкий» в случае применения тотального шифрования трафика между ИВК и всеми ПУ и УСПД. Дополнительно должны применяться меры сетевой безопасности ИВК, безопасного дизайна программного обеспечения ИВК, защиты ИВК от несанкционированного доступа, и другие меры безопасности, которые в совокупности выходят за пределы состава задач, рассматриваемых в настоящей модели угроз
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА					
4.1.5.1	Несанкционированная модернизация	С	Меры безопасности (регламент) выполнения ремонта и технического обслуживания ПУ и УСПД П30, П31. Штатная процедура ввода в эксплуатацию (регистрации) ПУ и УСПД после ремонта П22	Н	
4.1.5.2	Компрометация криптографических ключей устройства	С	Уничтожение криптографических ключей до передачи на техническое обслуживание и в ремонт П20, П22	П	
УГРОЗЫ ИБ ПУ, УСПД, СКЗИ ПУ и УСПД НА ЭТАПЕ УТИЛИЗАЦИИ					
4.1.6.1	Несанкционированная модернизация	С	Меры безопасности (регламент) выполнения утилизации ПУ, УСПД, СКЗИ ПУ и УСПД П32	Н	

Номер пункта	Способ реализации угрозы (атака)	Риск	Мера противодействия	Ост. риск	Примечание
4.1.6.2	Компрометация криптографических ключей устройства	С	Уничтожение криптографических ключей до передачи на утилизацию П20, П22	П	

5 ЗАКЛЮЧЕНИЕ ОБ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ УСПД, ПУ И СКЗИ УСПД И ПУ

В результате проведенного анализа угроз информационной безопасности УСПД, ПУ и СКЗИ УСПД и ПУ, можно сделать следующие выводы:

1 Применение приборов учета и устройств передачи данных, разработанных с учетом требований, установленных Правительством Российской Федерации для интеллектуальных систем учета электрической энергии (мощности) [2], порождает как новые угрозы, так и новые возможности комплексной защиты ПУ и УСПД в составе ИСУЭ. Важным фактором, существенно изменяющим условия безопасности эксплуатации ПУ и УСПД в терминах требований [2] является передача приборов учета и УСПД в руки единого, доверенного оператора ИСУЭ, что существенно ограничивает присутствие в числе пользователей ИСУЭ внутренних нарушителей. При правильной организации работы с персоналом оператора ИСУЭ к внутренним нарушителям можно отнести, в основном, только сотрудников сервисных организаций, обеспечивающих ввод в эксплуатацию, технологическое обслуживание и ремонт ПУ и УСПД.

2 Анализ угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД показывает, что внутренний нарушитель, обеспечивающий ввод в эксплуатацию, технологическое обслуживание и ремонт ПУ и УСПД, будет существенно ограничен в своих возможностях атаки на СКЗИ ПУ и УСПД в случае, если:

- идентификация ПУ и УСПД в течение всего их жизненного цикла будет осуществляться при помощи уникальных идентификаторов микроконтроллеров, применяемых в этих устройствах;

- контроль подлинности экземпляра ПУ и УСПД будет выполняться при помощи дополнительных некриптографических (транспортных) секретов,

формируемых в защищенных технологических процессах и исключающих возможность подмены изделия;

– целостность и аутентичность всего комплекса программного обеспечения, составляющего среду функционирования криптосредств ПУ и УСПД, будет контролироваться с использованием централизованных доверенных серверов ИСУЭ на этапах производства, ввода в эксплуатацию, ремонта ПУ и УСПД, будет исключена загрузка недоверенного программного обеспечения;

– все значимые технологические операции прошивки программного обеспечения, критичных данных и транспортных секретов будут выполняться при помощи специализированных автоматизированных рабочих мест, работающих совместно с доверенными серверами ИСУЭ и снабженных СКЗИ, сертифицированными ФСБ России, устойчивыми к атакам со стороны пользователя (класс СКЗИ не ниже КСЗ).

Важным следствием, вытекающим из предлагаемых для защиты от атак со стороны внутреннего нарушителя мер безопасности, является тот факт, что этот нарушитель не имеет возможности бесконтрольной работы с полнофункциональным СКЗИ. Дело в том, что СКЗИ не могут осуществлять свои функции без установленных криптографических ключей, а ПУ и УСПД на всех этапах, кроме этапа эксплуатации, не содержат в себе криптографических ключей, которые вводятся на этапе ввода устройства в эксплуатацию (операция персонализации СКЗИ) и уничтожаются при выводе устройства из эксплуатации.

Вместе с тем, для предупреждения атак со стороны внутреннего нарушителя, помимо применения СКЗИ класса не ниже КСЗ, должны быть дополнительно приняты следующие организационные меры безопасности:

а) требования безопасности должны быть в исчерпывающем составе перечислены в правилах пользования соответствующих СКЗИ, обеспечивающих производство, ввод в эксплуатацию (регистрацию), ремонт УСПД и ПУ, снабженных СКЗИ;

б) выполнять операции производства, ввода в эксплуатацию (регистрации) и ремонта УСПД и ПУ, снабженных СКЗИ, должен представитель организации, обладающей действующими лицензиями ФСБ России на выполнение соответствующих видов деятельности;

в) лицензиат ФСБ России, выполняющий операции производства, ввода в эксплуатацию (регистрации) и ремонта УСПД и ПУ, снабженных СКЗИ, должен:

1) разработать регламенты защищенных технологических процессов для исполнения всех операций, оказывающих влияние на состояние безопасности УСПД и ПУ, снабженных СКЗИ;

2) документировать все производственные, регистрационные и ремонтные операции с СКЗИ с указанием даты и времени, места исполнения операции технологического процесса, модели и серийного номера УСПД и ПУ, снабженного СКЗИ, с которым выполняется технологическая операция, регистрационного номера (регистрационных номеров) СКЗИ УСПД и ПУ, снабженных СКЗИ, регистрационного номера СКЗИ автоматизированного рабочего места, выполняющего технологическую операцию, результата технологической операции вне зависимости от успеха или неуспеха ее исполнения;

3) в установленном порядке предоставлять уполномоченным органам отчетность по деятельности, включая, при необходимости, первичные документы, описанные выше в перечислении б).

3 Другой важный вывод, вытекающий из анализа угроз информационной безопасности ПУ, УСПД, СКЗИ ПУ и УСПД, состоит в том, что в составе ИСУЭ эксплуатируются информационные активы существенно различные по ценности и по уровню ущерба от нарушения их информационной безопасности, в частности:

– риск нарушения конфиденциальности показаний приборов учета пренебрежимо мал; значительная часть сведений об энергопотреблении

абонентов сетей электроснабжения открыто читается прямо с индикаторов (дисплеев) ПУ и этот факт не беспокоит потребителей;

– нарушение целостности, потеря (уничтожение, компрометация, фальсификация) единичных показаний или даже полного потока показаний единичного прибора учета составляет, в масштабах ИСУЭ, пренебрежимо малый риск; наличие таких показаний и их достоверность относительно легко и достаточно эффективно контролируются со стороны ИВК, выстраивающего полный энергобаланс каждого объекта контроля и выявляющего все аномалии измерительного процесса ПУ (превышение или недостаток потребления, нарушения статистических показателей режимов потребления электрической энергии (мощности) во времени, соотношения между активной и реактивной составляющей мощности и т.п.);

– риск нарушения целостности, потери (уничтожения компрометации, фальсификации) показаний измерений, концентрируемых единичным УСПД, также изначально, даже без применения каких-либо средств защиты информации, оценивается как низкий по тем же причинам, что и для ПУ, а также потому, что единичное УСПД обслуживает относительно малое число (до нескольких сотен, в среднем - несколько десятков) ПУ;

– риски вмешательства в процесс конфигурирования ПУ и УСПД, не касающегося управления энергопотреблением, представляются низкими или средними;

– риски несанкционированного доступа к управлению энергопотреблением представляются высокими, поскольку могут приводить к экономическим потерям, нарушению хозяйственной деятельности и даже угрозам жизни и здоровью граждан, выступающих в качестве потребителей электроэнергии или зависящих от результатов деятельности потребителей электроэнергии;

– наивысшим же следует признать риск реализации угроз, выполняемых по типу инфраструктурных атак, связанных с массовыми нарушениями процесса энергоснабжения потребителей; ущерб от реализации таких угроз

сравним, а в ряде случаев может превосходить по техническим, экономическим, социальным и политическим последствиям, ущерб от крупных техногенных катастроф, экологических бедствий и террористических актов;

– инфраструктурные атаки могут иметь две цели: УСПД (ПУ) и ИВК; атаки на парк ПУ и УСПД могут приобретать реально опасные масштабы только в случае, если эти атаки осуществляются в массовых масштабах методами сетевого доступа; в то же время эффективная атака против ИВК может привести к катастрофическим последствиям в случае, если нарушителю удастся перехватить управление ИВК в целом; при этом важно понимать, что такая атака может быть осуществлена при помощи компрометированного ПУ или УСПД или от несанкционированно включенного в сеть под защитой УСПД вредоносного устройства; защита от атак на ИВК должна осуществляться, в первую очередь, средствами, локализованный в сетевом сегменте ИВК или на периметре этого сегмента; описание этих средств защиты выходит за пределы настоящей типовой модели угроз, однако важно понимать, что вероятность таких атак будет сведена к минимуму в случае, если каждый узел сети ИСУЭ, в том числе - каждый ПУ и УСПД будет снабжен СКЗИ, обеспечивающими режим взаимной аутентификации всех сетевых устройств и тотальной защиты (изолирующей политики шифрования трафика) ПУ и УСПД.

4 Анализ методов, которыми могут осуществляться различные угрозы показывает, что, по совокупности факторов, для ИСУЭ, представляющей собой территориально распределенную гетерогенную информационную систему массового обслуживания, являются сетевые информационные атаки. Этот вывод основывается на том, что:

– приборы учета и УСПД сами по себе достаточно хорошо защищены физически; традиция применения мер физической защиты распределительных, управляющих и измерительных приборов в энергетических сетях имеет более чем столетнюю историю и связана не только

с информационными атаками, но и с практикуемыми в течение десятилетий, со времен применения аналоговых систем, методами воровства энергоресурсов при помощи перекоммутаций, несанкционированных подключений, взлома устройств, воздействия на них электрическими полями, разрушения измерительных цепей, включения обходных контуров энергоснабжения и т.п. В этой связи в электроэнергетике давно наработаны практики физической защиты приборов, каналов подключения и коммутации, детектирования нарушений и реагирования на нарушения. Весь этот арсенал мер защиты физических устройств полностью применим к цифровым системам;

– цифровые системы, дополнительно к описанным методам защиты, добавляют существенно большую информативность сведений о практикуемых и даже подготавливаемых атаках и новые методы реагирования;

– процесс вскрытия защищенного корпуса устройства представляющего собой, по существу, периметр контролируемой зоны для применения ПУ, УСПД, СКЗИ ПУ и УСПД, трудоемок, требует применения инструментальных средств, выполняется в течение достаточно длительного времени, оставляет следы взлома и по всем перечисленным причинам связан с рисками обнаружения взломщика - как средствами информационных систем, так и средствами физической защиты приборов и устройств, внешними средствами охраны (оборудование допуска в подъезды, системы видеонаблюдения и т.п.) и непосредственно гражданами, потребителями электроэнергии, не заинтересованными в нарушениях процесса их электроснабжения;

– более того важно, что массовая реализация физических атак, описанных выше, не масштабируема; для того, чтобы реализовать или подготовить реализацию такой атаки, требуется массово применяемый человеческий ресурс, а для подготовки атаки на тысячи энергообъектов требуются недели и месяцы конспиративной работы подготовленных злоумышленников; сценарий такой «физической» инфраструктурной атаки

подобен одновременной организации сотен или тысяч военных диверсий и не посилен даже для высокоорганизованных групп нарушителей.

Напротив, компрометация массового парка ПУ и УСПД методами сетевого доступа, накопление из компрометированных устройств бот-сети, нацеленной на массовую инфраструктурную атаку, представляется не только реалистическим технически, но и соответствует практике подготовки и осуществления современных DOS- и DDOS-атак.

Таким образом, практически единственным методом противодействия практически единственной атаке на ИСУЭ, имеющей катастрофически тяжелые последствия, является обеспечение надежной сетевой защиты ПУ и УСПД при помощи средств криптографической защиты.

5 Важно отметить, что действенной мерой противодействия инфраструктурным атакам, полностью исключаящей зависимость такой атаки от состояния информационной безопасности ПУ и УСПД, является вывод криптографических ключей, разрешающих управление энергопотреблением, полностью за пределы для ПУ и УСПД. Эта цель может быть достигнута тем, что каждая команда управления энергопотреблением должна быть снабжена меткой времени и электронной подписью ИВК, сформировавшего данную команду. Команда подлежит исполнению в ПУ или УСПД только в том случае, если время исполнения команды соответствует текущему системному времени ИСУЭ плюс-минус короткий интервал допуска, а электронная подпись ИВК успешно проверена. Применение этой меры безопасности полностью независимо от всех видов атак, выполняемых на ПУ и УСПД, поскольку закрытый ключ электронной подписи ИВК содержится в доверенных серверах ИСУЭ и недостижим для нарушителя, выполняющего атаку на ПУ и УСПД.

6 Суммируя сказанное, для ПУ, УСПД, СКЗИ ПУ и УСПД, можно предложить следующий необходимый и достаточный состав мер (требований) информационной безопасности:

а) для защиты взаимодействий между ИВК и ПУ, ИВК и УСПД должны применяться средства криптографической защиты, обеспечивающие взаимную аутентификацию объектов взаимодействия, конфиденциальность и целостность данных, а также целостность потока сообщений, включая защиту от атаки повторной передачи сообщения. Для достижения целей безопасности ИСУЭ в ПУ и УСПД достаточно применения СКЗИ класса КС1, в то время, как в доверенных серверах ИСУЭ и в ИВК, в силу большого масштаба системы и критически важных задач управления ИСУЭ, необходимо применять СКЗИ класса не ниже КС3.

Выбор класса СКЗИ КС1 для УСПД и ПУ, снабженных СКЗИ, обоснован тем, что и в базовой модели угроз безопасности информации интеллектуальной системы учёта электрической энергии [3], и в анализе угроз информационной безопасности УСПД и ПУ, снабженных СКЗИ, на стадии их эксплуатации актуальными признаются угрозы со стороны внешнего нарушителя, осуществляемые методами сетевого доступа. Угрозы со стороны внешнего нарушителя, осуществляемые методами физического воздействия, по результатам анализа признаются неактуальными в силу того, что от основных факторов этих угроз (вскрытие корпуса прибора, модернизация ПО, компрометация ключей, навязывание команды управления) принят комплекс надежных мер защиты (применение датчиков вскрытия корпуса, уничтожение криптографических ключей, короткий срок эксплуатации ключей, отсутствие внутри атакуемого прибора криптографического ключа, ответственного за защиту команды управления, проверка электронной подписи ИВК при исполнении команд управления энергопотреблением). Защита же от угроз со стороны внутренних нарушителей, выполняющих операции производства, ввода в эксплуатацию (регистрации) и ремонта УСПД и ПУ, снабженных

СКЗИ, должна обеспечиваться при помощи соответствующих автоматизированных рабочих мест, снабженных СКЗИ класса не ниже КСЗ;

б) для достижения целей автономной эксплуатации ПУ и УСПД в течение назначенного срока эксплуатации не представляется возможным создание криптографических ключей со сроком жизни равным назначенному сроку эксплуатации ПУ и УСПД. Это связано с фундаментальными причинами, по которым сертификат на СКЗИ выдается на срок не более трех лет, что намного меньше назначенного срока эксплуатации ПУ и УСПД. Ограничение срока действия сертификата связано с тем, что в динамично изменяющемся мире информационных технологий никто не может прогнозировать срок сохранения стойкости средств защиты на период, превышающий срок действия сертификата СКЗИ. В этих условиях представляется равно необоснованным и предположение о том, что СКЗИ любого класса, соответствующее любому набору требований обеспечит сохранность криптографических ключей в течение срока, превышающего срок действия сертификата СКЗИ, а продление срока действия сертификата СКЗИ на период назначенного срока эксплуатации ПУ и УСПД представляется на текущий момент методически не подготовленным и, следовательно, не обоснованным. В этих условиях нет альтернативы тому, чтобы в течение назначенного срока эксплуатации ПУ и УСПД выполнялись следующие согласованные меры безопасности:

1) выполнялась последовательно разработка и обновление сертифицированных программных СКЗИ, сменяющих друг друга по мере истечения срока действия сертификата СКЗИ;

2) процесс обновления версий СКЗИ в течение назначенного срока эксплуатации ПУ и УСПД (по уровням рисков информационной безопасности не менее критичный, чем смена ключевого материала) должен быть защищен при помощи СКЗИ, подлежит оценке влияния;

3) теми же средствами криптографической защиты должен быть обеспечен и процесс загрузки и обновления программного обеспечения,

составляющего среду функционирования криптосредств ПУ и УСПД, подпадающую под оценку влияния;

4) формировался обновляемый связанный поток криптографических ключей, используемых для аутентификации участников защищенного взаимодействия; в качестве мер защиты данного потока ключей следует установить требования:

- максимального использования для генерации ключей аутентификации СКЗИ ПУ и УСПД энтропии, формируемой как в ПУ (УСПД), так и на доверенных серверах ИСУЭ;

- связывания криптографических ключей в потоке, невозможность навязать внешний ключ нарушителя в процессе обновления криптографических ключей аутентификации ПУ и УСПД;

- рационального (на уровне 1 – 3 месяцев) сокращения сроков применения криптографических ключей аутентификации;

- применения непосредственно для защиты трафика не ключей аутентификации, а диверсифицированных сеансовых ключей.

в) ПУ и УСПД должны быть снабжены надежными средствами физической защиты, позволяющими сформировать контролируемую зону применения СКЗИ внутри корпуса устройства или в монтажном шкафу, в котором размещается устройство. СКЗИ ПУ и УСПД должны быть прямо связаны с датчиками средств физической защиты ПУ и УСПД и должны обеспечивать уничтожение криптографических ключей в случае нарушения контролируемой зоны. ПУ и УСПД, прошедшие через процедуру уничтожения криптографических ключей, подлежат выводу из эксплуатации и регламентной ремонтной процедуре;

г) ПУ, УСПД, СКЗИ ПУ и УСПД должны производиться в защищенном технологическом процессе, гарантирующем целостность их структуры, уникальную идентификацию устройств, запись необходимых для подтверждения идентификации некриптографических (транспортных) секретов. СКЗИ ПУ и УСПД должны выпускаться с производства без записи

в них криптографических ключей. Производство ПУ, УСПД, СКЗИ ПУ и УСПД должно выполняться с применением сертифицированных ФСБ России как СКЗИ КСЗ;

д) ввод в эксплуатацию ПУ и УСПД должен сопровождаться персонализацией встроенных СКЗИ и созданием необходимых криптографических ключей. Ввод в эксплуатацию ПУ, УСПД, СКЗИ ПУ и УСПД должен выполняться при помощи специализированных автоматизированных рабочих мест, сертифицированных ФСБ России как СКЗИ КСЗ;

е) процесс эксплуатации ПУ и УСПД должен выполняться в автономном режиме с применением комплекса мер информационной безопасности, описанной в настоящей Модели угроз. При этом важнейшей мерой защиты ПУ и УСПД и ИСУЭ в целом является комплекс описанных мер сетевой информационной безопасности, исключающих в совокупности перехват управления энергопотреблением со стороны ИВК, компрометацию массовых парков ПУ, УСПД, СКЗИ ПУ и УСПД и приводящих к возможности выполнения инфраструктурных атак, связанных с массовым отключением потребителей от энергоснабжения. Важнейшим фактором защиты от упомянутых сетевых угроз является обеспечение режима полного шифрования и аутентификации всех обменов между ИВК и ПУ и УСПД. Этот режим защиты представляется более строгим, чем предписанный действующим в настоящее время стандартом [10], однако не входит в противоречие с требованиями данного стандарта и, одновременно, практически исключает возможность реализации большинства сетевых атак, включая инфраструктурные атаки на массовые парки ПУ и УСПД, а также атаки на ИВК, в том числе при помощи вредоносного устройства, включенного в сеть ИСУЭ;

ж) процесс эксплуатации ПУ и УСПД подлежит непрерывному контролю событий информационной безопасности, как локальному, выполняемому изнутри контуров физической защиты (контролируемых зон) ПУ и УСПД, так и внешнему, со стороны ИВК;

и) в случаях выявления угроз и инцидентов безопасности, в первую очередь при нарушении мер физической защиты ПУ и УСПД, СКЗИ ПУ и УСПД должны выполнять уничтожение криптографических ключей, ПУ и УСПД должны выводиться из эксплуатации и передаваться на регламентную ремонтную процедуру;

к) ремонтная процедура должна выполняться с ПУ и УСПД, СКЗИ которых не содержат криптографических ключей. Завершаться ремонтная процедура должна теми же мерами защиты, которыми завершается процесс производства ПУ и УСПД (см. перечисление г)). При выполнении ремонтных процедур должны использоваться СКЗИ аналогичные тем, которые используются при производстве ПУ, УСПД, СКЗИ ПУ и УСПД. По завершении ремонтной процедуры СКЗИ ПУ и УСПД не должны иметь криптографических ключей и при послеремонтном вводе в эксплуатацию должны пройти штатную регламентную процедуру, описанную в перечислении д).

Выполнение вышеперечисленных мер информационной безопасности должно обеспечить как выполнение эксплуатационных требований, устанавливаемых Министерством энергетики Российской Федерации, так и владельца ИСУЭ, при надлежащей, адекватной уровню угроз, степени защиты ИСУЭ и при разумном уровне затрат на достижение требуемого уровня информационной безопасности системы.

ПРИЛОЖЕНИЕ А

(справочное)

Источники разработки

1 Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике», в редакции Федерального закона от 27.12.2018 № 522-ФЗ.

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

3 Министерство энергетики Российской Федерации. «Базовая модель угроз безопасности информации интеллектуальной системы учёта электрической энергии». Введено в действие 29.06.2021 письмом НШ-7491/07 «О базовой модели угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности)».

4 Федеральная служба безопасности Российской Федерации. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утверждено приказом ФСБ России от 09.02.2005 № 66, зарегистрировано в Минюсте России 03.03.2005 № 6382.

5 ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

6 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

7 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

8 ГОСТ Р 51897-2021 «Менеджмент риска. Термины и определения».

9 ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

10 ГОСТ Р 58940-2020 «Требования к протоколам обмена информацией между компонентами интеллектуальной системы учета и приборами учета».

11 МР 26.4.003-2019 «Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу dîms». (ТК 26, протокол № 24 от 14.11.2019).

12 Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

к базовой модели угроз безопасности информации
интеллектуальной системы учета электрической энергии

**ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ
КОМПОНЕНТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УЧЕТА
ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ**

ВАРИАНТ 3

Типовая модель угроз программных (программно-аппаратных) средств криптографической защиты информации, применяемых для защиты информационно-вычислительных комплексов электроустановки (устройств сбора и передачи данных) и приборов учета в интеллектуальных системах и средств учёта электрической энергии (мощности) с трехуровневой структурно-коммуникационной схемой

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	4
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	5
НОРМАТИВНЫЕ ССЫЛКИ.....	7
1 ОБЩИЕ ПОЛОЖЕНИЯ.....	8
1.1 Назначение частной модели угроз	8
1.2 Цели разработки частной модели угроз	8
1.3 Объекты защиты.....	8
1.4 Структура модели угроз	9
2 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА И СРЕДЫ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЗАЩИТЫ И ЦЕЛЕЙ БЕЗОПАСНОСТИ	10
2.1 Структура функциональных объектов защиты информации	10
2.2 Описание жизненного цикла ивк, пу, успд.....	19
2.3 Описание жизненного цикла скзи пу, скзи успд и скзи ивк	26
3 МОДЕЛЬ НАРУШИТЕЛЯ ИБ УСПД, ПУ, ИВК, СКЗИ УСПД, СКЗИ ПУ И СКЗИ ИВК	29
3.1 Внешний нарушитель пу и скзи пу	30
3.2 Внутренний нарушитель пу и скзи пу	33
3.3 Внешний нарушитель успд и скзи успд	33
3.4 Внутренний нарушитель успд и скзи успд.....	36
3.5 Внешний нарушитель ивк и скзи ивк	37
3.6 Внутренний нарушитель ивк и скзи ивк.....	39
4 МОДЕЛЬ УГРОЗ ИБ УСПД И ПУ	41
4.1 Состав и описание угроз иб ивк, успд, пу, скзи пу, скзи успд, скзи ивк.....	41
4.2 Классификация угроз иб ивк, успд, пу, скзи пу, скзи успд, скзи ивк	43

4.3 Описание мер противодействия угрозам иб ивк, успд, пу, скзи пу, скзи успд, скзи ивк и оценка эффективности мер противодействия угрозам иб ивк, успд, пу, скзи пу, скзи успд, скзи ивк	44
4.4 Уточнение предположения об актуальных нарушителях	47
5 ЗАКЛЮЧЕНИЕ ОБ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	48

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место
АС	– автоматизированная система
ВПО	– вредоносное программное обеспечение
ИБ	– информационная безопасность
ИВК	– информационно-вычислительный комплекс
ИВКЭ	– информационно-вычислительный комплекс электроустановки
ИСУЭ	– интеллектуальные системы учета электроэнергии(мощности)
КЗ	– контролируемая зона
КИ	– ключевая информация
КИИ	– критическая информационная инфраструктура
MITM	– Man in the middle – атака «человек посередине»
НДВ	– недекларированные возможности
НСД	– несанкционированный доступ
ПУ	– прибор учета электрической энергии
СКЗИ	– средство криптографической защиты информации
СФ	– среда функционирования
УСПД	– устройство сбора и передачи данных
УБИ	– угрозы безопасности информации
ЧМУ	– частная модель угроз

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.

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

Доступ к информации – возможность получения информации и ее использования.

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.

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 иницируемый 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.

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.

НОРМАТИВНЫЕ ССЫЛКИ

В настоящем документе использованы нормативные ссылки на следующие документы:

– «Базовая модель угроз безопасности информации интеллектуальной системы учета электрической энергии»

[<https://minenergo.gov.ru/view-pdf/20966/158908>];

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

[<http://static.government.ru/media/acts/files/1202006230034.pdf>];

– Приказ ФСБ России от 10.07.2014 №378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

[https://www.consultant.ru/document/cons_doc_LAW_167862/3faa8723e46ecc4973f2bc794c221b88debfcaa9/];

– Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности от 31.03.2015 № 149/7/2/6-432

[http://www.fsb.ru/files/PDF/Metodicheskie_recomendacii.pdf].

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение частной модели угроз

Настоящая частная модель угроз (далее – ЧМУ) подготовлена в соответствии с «Базовой моделью угроз безопасности информации интеллектуальной системы учета электрической энергии (мощности)» (далее – Модель угроз), утвержденной Министерством энергетики Российской Федерации (далее – Минэнерго России).

Настоящая ЧМУ предназначена для постановки задач и разработки требований по информационной безопасности интеллектуальных систем учета электроэнергии (мощности) (ИСУЭ) и их компонентов: приборов учета (ПУ), устройств сбора и передачи данных (УСПД) и информационно-вычислительных комплексов (ИВК).

1.2 Цели разработки частной модели угроз

Целями разработки настоящей ЧМУ являются:

- изучение состава объектов защиты, а также состав функций (механизмов) информационной безопасности, возможностей нарушителей безопасности информации, обрабатываемой устройствами сбора и передачи данных и приборами учета электрической энергии с применением средств криптографической защиты информации;
- определение уровня защиты объектов защиты, а также состава функций (механизмов) информационной безопасности средств криптографической защиты информации, которые должны обеспечивать компенсацию угроз (рисков) информационной безопасности компонентов ИСУЭ на всех этапах жизненного цикла;
- оценка эффективности предлагаемых средств (мер, механизмов) информационной безопасности средств криптографической защиты информации компонентов ИСУЭ.

1.3 Объекты защиты

Объектами защиты являются:

- команды от ИВК;
- показания приборов и служебная передаваемая информация;
- ключевая информация, находящаяся в СКЗИ;
- ПО СКЗИ;
- средства, сопутствующие СКЗИ, в том числе:

- АРМ персонализации, предназначенное для проведения работ по загрузке конфигурационных параметров и сертификатов в СКЗИ перед введением его в эксплуатацию;
 - Сервер генерации, предназначенный для ведения базы производства и хранения данных о сериях, производимых СКЗИ;
 - АРМ инициализации, предназначенное для управления оборудованием при производстве СКЗИ;
- технические средства, в которые встраиваются СКЗИ (ИВК, УСПД, ПУ).

Примечание – Средства, сопутствующие СКЗИ, функционируют на предприятиях изготовителях, порядок эксплуатации данных СКЗИ определяется правилами пользования, подлежащими согласованию с ЦЗИСС ФСБ России.

1.4 Структура модели угроз

- описание информационной системы;
- структурно-функциональные характеристики;
- описание угроз безопасности;
- модель нарушителя;
- возможные уязвимости;
- способы реализации угроз;
- последствия от нарушения свойств безопасности информации.

2 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА И СРЕДЫ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЗАЩИТЫ И ЦЕЛЕЙ БЕЗОПАСНОСТИ

2.1 Структура функциональных объектов защиты информации

2.1.1 Структура ИСУЭ

ИСУЭ построена по клиент-серверной архитектуре и может иметь в соответствии с выполняемыми функциями три функциональных уровня, объединенных 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;

- устройство сбора и передачи данных (далее — УСПД) — находящаяся 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;

Примечание – для среднего уровня ИСУЭ в терминологии «Базовой модели угроз безопасности информации интеллектуальной системы учета электрической энергии (мощности)», утвержденной Министерством энергетики Российской Федерации применяется обозначение «ИВКЭ».

- приборы учета электрической энергии (далее — ПУ) — находящиеся на нижнем уровне ИСУЭ средства измерения, представляющие 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).

2.1.2 Требования и компоненты ИСУЭ, образующие среду функционирования ИВК, ПУ и УСПД

Требования к ИСУЭ устанавливаются следующими пунктами Постановления Правительства РФ от 19 июня 2020 г. N 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)»:

2.1.2.1 пункт 28

Прибор учета электрической энергии, который может быть присоединен к интеллектуальной системе учета, должен удовлетворять требованиям, предъявляемым законодательством Российской Федерации об обеспечении единства измерений к средствам измерений, применяемым в сфере государственного регулирования обеспечения единства измерений, и обеспечивать в точке учета:

- ведение времени независимо от наличия напряжения в питающей сети с абсолютной погрешностью хода внутренних часов не более 5 секунд в сутки, а также с возможностью смены часового пояса;

- возможность синхронизации и коррекции времени с внешним источником сигналов точного времени;

- контроль наличия внешнего переменного и постоянного магнитного поля;

- отображение на встроенном и (или) выносном цифровом дисплее:

- текущих даты и времени;
- текущих значений потребленной электрической энергии суммарно и по тарифным зонам;
- текущих значений активной и реактивной мощности, напряжения, тока и частоты;
- значения потребленной электрической энергии на конец последнего программируемого расчетного периода суммарно и по тарифным зонам;
- индикатора режима приема и отдачи электрической энергии;
- индикатора факта нарушения индивидуальных параметров качества электроснабжения;
- индикатора вскрытия электронных пломб на корпусе и клеммной крышке прибора учета электрической энергии;
- индикатора факта события воздействия магнитных полей со значением модуля вектора магнитной индукции

свыше 150 мТл (пиковое значение) на элементы прибора учета электрической энергии;

- индикатора неработоспособности прибора учета электрической энергии вследствие аппаратного или программного сбоя.

– индикацию функционирования (работоспособного состояния) на корпусе и выносном дисплее (при наличии выносного дисплея);

– наличие 2 интерфейсов связи для организации канала связи (оптического и иного другого), а в отношении приборов учета электрической энергии трансформаторного включения также по цифровому электрическому интерфейсу связи RS-485 или цифровому электрическому интерфейсу связи Ethernet;

– защиту прибора учета электрической энергии от несанкционированного доступа с помощью реализации в приборе учета:

- идентификации и аутентификации;
- контроля доступа;
- контроля целостности;
- регистрации событий безопасности в журнале событий.

– фиксирование несанкционированного доступа к прибору учета посредством энергонезависимой электронной пломбы, фиксирующей вскрытие клеммной крышки и вскрытие корпуса (для разборных корпусов);

– фиксацию воздействия постоянного или переменного магнитного поля с указанием даты и времени воздействия со значением модуля вектора магнитной индукции свыше 150 мТл (пиковое значение);

– запись событий в отдельные выделенные сегменты энергонезависимой памяти прибора учета электрической энергии (с указанием даты и времени), результатов нарушения индивидуальных параметров качества электроснабжения - в отдельные выделенные сегменты энергонезависимой памяти прибора учета электрической энергии (далее соответственно - журнал событий, ведение журнала событий) в объеме не менее чем на 500 записей;

– ведение журнала событий, в котором должно фиксироваться следующее:

- дата и время вскрытия клеммной крышки;
- дата и время вскрытия корпуса прибора учета электрической энергии (для разборных корпусов);
- дата, время и причина включения и отключения встроенного коммутационного аппарата;
- дата и время последнего перепрограммирования;
- дата, время, тип и параметры выполненной команды;

- попытка доступа с неуспешной идентификацией и (или) аутентификацией;
- попытка доступа с нарушением правил управления доступом;
- попытка несанкционированного нарушения целостности программного обеспечения и параметров;
- изменение направления перетока мощности (для однофазных и трехфазных приборов учета электрической энергии);
- дата и время воздействия постоянного или переменного магнитного поля со значением модуля вектора магнитной индукции свыше 150 мТл (пиковое значение) с визуализацией индикации;
- факт связи с прибором учета электрической энергии, приведшей к изменению параметров конфигурации, режимов функционирования (в том числе введение полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии (управление нагрузкой);
- дата и время отклонения напряжения в измерительных цепях от заданных пределов;
- отсутствие или низкое напряжение при наличии тока в измерительных цепях с конфигурируемыми порогами (кроме однофазных и трехфазных приборов учета электрической энергии прямого включения);
- отсутствие напряжения либо значение напряжения ниже запрограммированного порога по каждой фазе с фиксацией времени пропадания и восстановления напряжения;
- инверсия фазы или нарушение чередования фаз (для трехфазных приборов учета электрической энергии);
- превышение соотношения величин потребления активной и реактивной мощности;
- небаланс тока в нулевом и фазном проводе (для однофазных приборов учета электрической энергии);
- превышение заданного предела мощности.

– формирование по результатам автоматической самодиагностики обобщенного события или каждого факта события;

– изменение текущих значений времени и даты при синхронизации времени с фиксацией в журнале событий времени до и после коррекции или величины коррекции времени, на которую было скорректировано значение;

– возможность 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 (кроме приборов учета электрической энергии трансформаторного включения), в следующих случаях:

- запрос интеллектуальной системы учета;
- превышение заданных в приборе учета электрической энергии пределов параметров электрической сети;
- превышение заданного в приборе учета электрической энергии предела электрической энергии (мощности);
- несанкционированный доступ к прибору учета электрической энергии (вскрытие клеммной крышки, вскрытие корпуса (для разборных корпусов) и воздействие постоянным и переменным магнитным полем).

– возобновление подачи электрической энергии по запросу интеллектуальной системы учета, в том числе путем фиксации встроенного коммутационного аппарата в положении «включено» непосредственно на приборе учета электрической энергии;

– обеспечение энергонезависимого хранения журнала событий, выявление фактов изменения (искажения) информации, влияющих на информацию о количестве и иных параметрах электрической энергии, а также фактов изменения (искажения) программного обеспечения прибора учета электрической энергии;

– возможность организации с использованием защищенных протоколов передачи данных из состава протоколов, утвержденных Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с Министерством энергетики Российской Федерации, информационного обмена с интеллектуальной системой учета, в том числе передачи показаний, предоставления информации о результатах измерения количества и иных параметров электрической энергии, передачи журналов событий и данных о параметрах настройки, а также удаленного управления

прибором учета электрической энергии, не влияющих на результаты выполняемых приборами учета электрической энергии измерений, включая:

- корректировку текущей даты и (или) времени, часового пояса;
- изменение тарифного расписания;
- программирование состава и последовательности вывода сообщений и измеряемых параметров на дисплей;
- программирование параметров фиксации индивидуальных параметров качества электроснабжения;
- программирование даты начала расчетного периода;
- программирование параметров срабатывания встроенных коммутационных аппаратов;
- изменение паролей доступа к параметрам;
- изменение ключей шифрования;
- управление встроенным коммутационным аппаратом путем его фиксации в положении «отключено» (кроме приборов учета электрической энергии трансформаторного включения).

– возможность передачи зарегистрированных событий в интеллектуальную систему учета по инициативе прибора учета электрической энергии в момент их возникновения и выбор их состава.

2.1.2.2 пункт 29

Для приборов учета электрической энергии непосредственного включения необходимо наличие возможности физической (аппаратной) блокировки срабатывания встроенного коммутационного аппарата, используемого для полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии, приостановления или ограничения предоставления коммунальной услуги (управление нагрузкой). Реализация физической (аппаратной) блокировки должна сопровождаться процессом опломбирования.

2.1.2.3 пункт 38

Защита интеллектуальной системы учета и содержащейся в ней информации должна обеспечиваться в соответствии с федеральными законами «О персональных данных», «О безопасности критической информационной инфраструктуры Российской Федерации», «Об информации, информационных технологиях и о защите информации» и актами Федеральной службы безопасности Российской Федерации, разработанными в соответствии с подпунктом «ш» статьи 13 Федерального закона

«О федеральной службе безопасности», путем принятия организационных и технических мер, а также в соответствии с настоящими Правилами.

2.1.2.4 пункт 39

Необходимость шифрования (применение средств криптографической защиты) информации при ее передаче по каналам связи интеллектуальной системы учета определяется субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, самостоятельно.

При определении субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, необходимости шифрования (применения средств криптографической защиты) информации при ее передаче по каналам связи интеллектуальной системы учета рекомендуется руководствоваться базовой моделью нарушителя (моделью угроз безопасности информации), размещенной на официальном сайте Министерства энергетики Российской Федерации в информационно-телекоммуникационной сети «Интернет».

2.1.2.5 пункт 40

В целях определения актуальных угроз безопасности информации, обрабатываемой в интеллектуальных системах учета, субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, могут быть разработаны частные модели нарушителя (модели угроз безопасности информации).

При разработке частных моделей нарушителя (моделей угроз безопасности информации) рекомендуется использовать базовую модель нарушителя (модель угроз безопасности информации) в интеллектуальных системах учета, размещаемую на официальном сайте Министерства энергетики Российской Федерации в информационно-телекоммуникационной сети «Интернет».

2.1.2.6 пункт 41

В случае, когда субъектом электроэнергетики, являющимся владельцем интеллектуальной системы учета, определена потребность в криптографической защите информации, обрабатываемой в такой системе, рекомендуется применять средства криптографической защиты информации, прошедшие процедуру оценки соответствия требованиям, предъявляемым федеральным органом исполнительной власти в области обеспечения безопасности.

Сертифицированные средства защиты информации применяются в случаях, установленных законодательством Российской Федерации о техническом регулировании.

2.1.2.7 пункт 42

Принимаемые меры по защите интеллектуальной системы учета и содержащейся в ней информации должны в том числе обеспечивать:

- механизмы идентификации и аутентификации по логину и паролю в каждом из компонентов и элементов интеллектуальной системы учета с обязательной фиксацией в интеллектуальной системе учета информации о неверном вводе пароля;
- предотвращение неправомерного доступа к информации, обрабатываемой и хранимой в интеллектуальной системе учета и приборах учета электрической энергии, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение воздействия на технические и программные средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование интеллектуальной системы учета;
- восстановление функционирования интеллектуальной системы учета в том числе за счет резервирования информации и (или) технических средств обработки информации, каналов связи;
- контроль доступа пользователей к данным и операциям в интеллектуальной системе учета;
- своевременное обнаружение фактов несанкционированного доступа к интеллектуальной системе учета и содержащейся в ней информации.

2.1.2.8 пункт 43

Прибор учета электрической энергии не должен иметь возможность управления ограничением нагрузки другими элементами интеллектуальной системы учета и другими приборами учета электрической энергии (не должен инициировать управляющие сигналы и воздействия).

2.1.2.9 пункт 44

Допускается ретрансляция одним прибором учета электрической энергии сигналов управления, полученных им с промежуточного элемента интеллектуальной системы учета и адресованных другим приборам учета электрической энергии, в случае его функционирования в режиме ретрансляции.

Данные требования были дополнительно разъяснены Министерством энергетики Российской Федерации в письме от 16.07.2021 № СП-8400/07 «Об СКЗИ для интеллектуальных систем учета электрической энергии», в котором, в частности говорится:

«...необходимо в состав типовых функциональных и эксплуатационных требований к СКЗИ включить следующие требования:

- назначенный срок эксплуатации СКЗИ для ИВКЭ должен быть не менее 16 лет;

- СКЗИ для ИВКЭ должны иметь непрерывно действующие сертификаты соответствия, выданные ФСБ России, в течение всего назначенного срока эксплуатации;

- СКЗИ для ИВКЭ должны обеспечивать возможность дистанционного обновления их программного обеспечения, в том числе в целях их приведения в соответствие с новыми требованиями по безопасности информации, которые могут быть приняты в течение их назначенного срока эксплуатации;

- СКЗИ для ИВКЭ должны обеспечивать возможность дистанционного обновления программного обеспечения ИВКЭ;

- для эксплуатации СКЗИ для ИВКЭ не требуется создания контролируемой зоны, выходящей за пределы корпуса ИВКЭ, подлежащих защите с использованием СКЗИ, а также дополнительных средств контроля доступа в составе СКЗИ для ИВКЭ, помимо предусмотренных Правилам предоставления доступа к ИСУ;

- СКЗИ для ИВКЭ не должны требовать особых условий размещения на объектах потребителей;

- в правилах пользования СКЗИ должен быть разработан сценарий действий владельца ИСУ в случае компрометации ключа шифрования СКЗИ для ИВКЭ в момент эксплуатации, не приводящий к кардинальной замене всего оборудования ИСУ;

- СКЗИ для ИВКЭ должны обеспечивать возможность их эксплуатации без необходимости физического доступа к ним, в том числе без замены их аппаратных частей, в течение всего назначенного срока эксплуатации;

- СКЗИ для ИВКЭ должны обеспечивать совместимость всех экземпляров изделий, подключенных к ИСУ, независимо от объекта их размещения;

- СКЗИ для ИВКЭ должны обеспечивать совместимость с программно-аппаратными средствами, применяемыми в элементах ИСУ, подлежащих защите с использованием СКЗИ;

- встраивание СКЗИ для ИВКЭ должно нести минимальные издержки по времени и затратам для производителей ИВКЭ и не должно оказывать существенного влияния на технологический процесс производства;

- СКЗИ, предназначенные для использования в составе ИСУ, должны быть совместимы с программно-аппаратными средствами действующих ИСУ;

- в СКЗИ должна быть реализована и функция шифрования, и функция электронной подписи;

- СКЗИ не должны предъявлять дополнительные требования к персоналу;

- СКЗИ для ИВКЭ должно быть реализовано в виде аппаратного средства СКЗИ или в виде программного обеспечения СКЗИ.

- Кроме того, необходимо в состав типовых функциональных и эксплуатационных требований к СКЗИ рассмотреть возможность включения требований по дистанционной загрузке ключей в СКЗИ для ИВКЭ после их установки на объекте потребителя, а также дистанционного обновления ключей в СКЗИ для ИВКЭ в течение всего назначенного срока эксплуатации»

- «Одновременно полагаем целесообразным рассмотреть возможность предъявления к СКЗИ для ИСУ таких требований по безопасности информации, при которых деятельность по разработке и производству элементов ИСУ, подлежащих защите с использованием СКЗИ, а также деятельность по их установке и ремонту на объектах потребителей могла бы осуществляться соответствующими организациями без необходимости получения лицензий на деятельность с шифровальными (криптографическими) средствами».

2.2 Описание жизненного цикла ИВК, ПУ, УСПД

2.2.1 Этап производства

2.2.1.1 Планирование, разработка ТЗ, спецификация требований

На данном этапе определяются назначение конечного продукта, его технические характеристики, показатели качества и технико-экономические требования, предписание по выполнению необходимых стадий создания документации и её состав, а также специальные требования.

2.2.1.2 Требования по безопасности

При разработке определяются требования по безопасности, предъявляемые к разрабатываемому Изделию.

В качестве источников для формирования требований используются требования законов, нормативных правовых актов, отраслевых стандартов, требования заказчика и сценарии эксплуатации Изделия.

Требования по безопасности могут быть отражены в техническом задании, которое разрабатывается в соответствии с ГОСТ IEC 60950-1-2011 «Оборудование информационных технологий. Требования безопасности» (в настоящее время заменен ГОСТ IEC 60950-1-2014), ГОСТ 19.201-78 «ЕСПД. Техническое задание. Требования к содержанию и оформлению», ГОСТ Р 51317.6.5-2006 «Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых на электростанциях и подстанциях. Требования и методы испытаний».

2.2.1.3 Проект архитектуры разрабатываемого изделия

При разработке продукции создается документированный проект архитектуры Изделия. Поскольку Изделие включает в себя встроенное программное обеспечение, также создается проект архитектуры программы, который может быть представлен в описании программы (ГОСТ 19.402-78) и в пояснительной записке (ГОСТ 19.404-79).

2.2.1.4 Разработка

Каждому участнику группы разработки назначается задача из списка работ. После выполнения назначенного задания участник команды приступает к следующему.

2.2.1.5 Используемые инструментальные средства

В ходе работы по разработке продукта используются только идентифицированные инструментальные средства с определенными настройками (опциями).

К инструментальным средствам относятся: трансляторы, компиляторы, прикладные программы, используемые для проектирования и документирования, редакторы исходного кода программ, отладчики, интегрированные среды разработки; средства для разработки аппаратной части Изделия.

Для каждого инструментального средства определены:

- наименование и идентификационные признаки;
- наименование разработчика;
- ссылка на эксплуатационные документы;
- значения, применяемые при создании программы, опции (настройки).

2.2.1.6 Прослеживаемость соответствия изделия проектам компонентов архитектуры изделия

При создании Изделия его разработчик основывается на проектах компонентов архитектуры, которые определяются в ходе процессов проектирования.

Документация на Изделие содержит сведения о прослеживаемости соответствия проектам компонентов архитектуры Изделия.

2.2.1.7 Порядок оформления исходного кода программы

При создании программ исходный код оформляется в соответствии с определенным порядком. В случае невозможности использования порядка оформления исходного кода программы разработчик в документированном виде пишет обоснование факта отказа от использования принятого порядка оформления. Документирование производится в форме комментариев в исходном коде программы.

2.2.1.8 Статический анализ и экспертиза исходного кода программы

Разработчик ПО проводит статический анализ и экспертизу исходного кода программы с целью выявления недостатков программы, потенциально уязвимых конструкций в исходном коде программы. По результатам статического анализа и экспертизы исходного кода программы может проводиться доработка программы.

2.2.1.9 Тестирование

На этапе активной разработки продукта проводится:

- функциональное тестирование закрытых требований/улучшений – выполняется тестировщиками с использованием сборок программного продукта, выходящих с периодичностью, установленной командой разработки;

- регрессионное тестирование решённых ошибок – выполняется тестировщиками после каждой сборки программного продукта.

- нагрузочное тестирование – выполняется, если есть техническая возможность, и к началу этапа тестирования есть условно стабильная сборка.

На этапе тестирования продукта (после окончания этапа разработки) разово проводятся:

- полный прогон системы;

- регрессионное тестирование – проводится тестирование решённых ошибок (выполняется тестировщиками после каждой сборки программного продукта);

- нагрузочное тестирование;

- тестирование совместимости – проверка работоспособности продукта в заданном окружении конфигурации оборудования, набора стороннего программного обеспечения и набора данных;

- Beta-тестирование – заказчику предоставляется Beta-версия дистрибутива для тестирования на тестовых стендах заказчика и предоставления обратной связи по найденным ошибкам или предложениями по доработкам.

2.2.1.10 Критерии готовности продукта

Факт готовности продукта определяется на этапе тестирования при проведении полного прогона. Критериями готовности выступают:

- отсутствие критических и важных ошибок после последнего проведенного полного прогона;
- отсутствие превышения допустимого количества ошибок с приоритетом «Желательный».

При положительном завершении внутренней приемки продукт передается на сертификацию/инспекционный контроль.

2.2.1.11 Сертификация изделия

Сертификация состоит из следующих шагов:

- оформление разработчиком Заявки в Федеральное агентство по техническому регулированию и метрологии на сертификацию;
- оформление Федеральным агентством по техническому регулированию и метрологии Решения на проведение сертификации;
- заключение разработчиком Договора с Испытательной лабораторией на проведение сертификационных испытаний;
- проведение Испытательной лабораторией сертификационных испытаний;
- оформление Испытательной лабораторией Протоколов сертификационных испытаний и Технических заключений;
- заключение Испытательной лабораторией Договора о проведении экспертизы результатов сертификационных испытаний в Органе по сертификации;
- экспертиза Органом по сертификации результатов сертификационных испытаний и передача во ФСТЭК России;
- оформление Сертификата Федеральным агентством по техническому регулированию и метрологии.

В группу завершающих процессов входят процессы, осуществляемые для формального завершения всех работ проекта, передачи готового продукта заказчикам и потребителям проекта или закрытия остановленного проекта.

Проект завершается сертификацией контролем и получением сертификата Федерального агентства по техническому регулированию и метрологии

2.2.1.12 Постановка изделия на производство

На данном этапе осуществляется подготовка и освоение производства, которые представляют собой этапы постановки продукции на производство. Постановка продукции осуществляется с целью обеспечения готовности производства к изготовлению и выпуску (поставке) вновь разработанной (модернизированной) продукции в заданном объеме, соответствующей всем установленным требованиям

2.2.2 Этап передачи

Передача изделия представляет собой продажу продукции заинтересованным лицам (заказчикам) из числа изготовленной.

Процедура передачи (поставки) Изделия пользователю обеспечивает безопасную передачу готовой продукции под ответственность пользователя.

В общем виде задачи, которые выполняются при поставке продукции (если не требуется разработка/доработки продукта), выглядят следующим образом:

- Определение/поиск приобретающей стороны;
- Рассмотрение требований, изложенных в заявке;
- Подготовка предложения в ответ на заявку;
- Согласование контракта: проведение переговоров для заключения контракта с приобретающей стороной на поставку продукции;

Поставка и поддержка продукта:

- Поставка продукта должна осуществляться в соответствии с требованиями контракта;
- Должно быть обеспечено содействие приобретающей стороне в поддержке поставленного продукта.

Закрытие работ:

- Принятие и подтверждение оплаты;
- Передача ответственности за продукт приобретающей стороне в порядке, предусмотренном в соглашении.

В процедурах поставки учитываются следующие вопросы:

- Обеспечение точного соответствия между продуктом, полученным потребителем, и прошедшим оценку;

- Избежание/обнаружение какой-либо подделки актуальной версии продукта;
- Предотвращение поставки фальсифицированной версии продукта;
- Избежание нежелательной утечки информации о поставке продукции заказчику;
- Избежание/обнаружение перехвата продукции во время поставки;
- Избежание задержки поставки или невыполнение поставки продукции.

Процедура передачи производится следующим образом:

- готовая продукция передается на склад готовой продукции;
- после поступления изделия на склад готовой продукции на такое изделие (или партию изделий) оформляются отгрузочные документы и производится транспортная упаковка;
- после оформления отгрузочных документов и упаковки изделия (или партии изделий) в транспортную упаковку в соответствии с заказом на производство производится отгрузка изделия заказчику через транспортную компанию.

Обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования, реализуется при помощи процедур верификации.

Для верификации продукта необходимо сверить номер версии полученного Изделия и маркировку с указанными значениями в Формуляре.

2.2.3 Этап установки

На этапе установки осуществляется установка Изделия на место эксплуатации.

Процедура установки включает в себя:

- механическая установка;
- подключение;
- пломбирование;
- заполнение «монтажной ведомости», в которой указывается связка заводского номера с местом установки.

Монтажные ведомости периодически (раз в день или по объему установки) передаются наладчикам на ИВК. Наладчик производит импорт данных из монтажной ведомости в ИВК после чего запускает опрос данных. Если в течение определенного времени (1-3 дня) прибор «не вышел на связь» информация передается монтажным бригадам для устранения.

Устранение заключается в повторном осмотре и выявлении причин неработоспособности. При выявлении неисправности Изделия происходит его замена.

Регистрация УСПД производится наладчиками на уровне ИВК.

2.2.3.1 Меры безопасности при использовании изделия:

Требования по безопасности при использовании изделия устанавливаются в соответствии с ГОСТ Р 51321.1-2007.

2.2.4 Этап эксплуатации

На этапе эксплуатации проводятся следующие процедуры:

2.2.4.1 Опрос ИСУЭ. Регламент опроса ИСУЭ определяет заказчик ИСУЭ.

2.2.4.2 Осмотр ИСУЭ. Периодически (примерно 1 раз в 12 месяцев) производятся осмотры компонентов ИСУЭ. Осмотры осуществляют работники эксплуатирующей организации (сетевая или сбытовая компания). Фиксируются только нарушения в подключении или в работе. Фиксация осуществляется посредством составления бумажного акта.

2.2.4.3 Поверка ПУ и УСПД. Межповерочный интервал ПУ составляет 16 лет. Межповерочный интервал УСПД составляет 10 лет.

2.2.5 Этап технического обслуживания

В течение срока действия гарантийных обязательств предприятие-изготовитель безвозмездно производит ремонт изделия или осуществляет его гарантийную замену при соблюдении потребителем условий хранения и эксплуатации, а также сохранности пломбы предприятия-изготовителя

2.2.6 Этап утилизации

Вышедшие из строя Изделия ремонтируются либо утилизируются в зависимости от степени повреждения. Отремонтированное оборудование возвращается заказчику для установки на объекты. На время ремонта заказчик использует оборудование из ЗИП. Ремонт производит завод изготовитель или специализированный сервисный центр. Оборудование, поступающее в ремонт, сопровождается официальным письмом или актами передачи (произвольной формы). При возврате из ремонта оформляются акты передачи. Если оборудование не подлежит ремонту, то оно возвращается заказчику с техническим актом экспертизы о не ремонтпригодности. В случае несоответствия технического уровня и качества выпускаемой продукции современным требованиям или освоения в производстве аналогичной по назначению новой продукции, имеющей более высокие технические и

технико-экономические показатели, в случае отсутствия заказов на поставку или потребительского спроса, в случае сокращения номенклатуры данного вида продукции в результате работ по унификации и прочее, принимается решение о снятии продукции с производства, что означает прекращение промышленного производства продукции.

2.3 Описание жизненного цикла СКЗИ ПУ, СКЗИ УСПД и СКЗИ ИВК

2.3.1 Этап разработки

Разработка СКЗИ производится в соответствии с «Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005).

СКЗИ разрабатываются в ходе ОКР по ТЗ, согласованному с ФСБ России. В соответствии с ТЗ и отдельно разработанной ПИМ проводятся тематические исследования на соответствие требованиям, предъявляемым к СКЗИ ФСБ России.

2.3.2 Этап производства

В СКЗИ используется асимметричная ключевая система на основе ключей ГОСТ 34.10-2018. СКЗИ использует объекты инфраструктуры открытого ключа (сертификаты, списки отозванных сертификатов и т.д.) стандарта X509, формируемые на сторонних удостоверяющих центрах, сертифицированных ФСБ России. СКЗИ имеют встроенный механизм контроля срока действия ключей. Срок действия приватных ключей в СКЗИ составляет 1 год.

СКЗИ реализуют следующие криптографические функции:

- хэширование согласно ГОСТ 34.11-2018/ ГОСТ Р 34.11-2012;
- генерация последовательностей случайных чисел (ПСЧ);
- генерация ключевых пар ГОСТ 34.10-2018/ ГОСТ Р 34.10-2012;
- создание, проверка ЭП согласно ГОСТ 34.10-2018./ ГОСТ Р 34.11-2012;
- шифрование по ГОСТ Р 34.12-2015 в режимах согласно ГОСТ Р 34.13-2015.

Плановая смена ключей производится в соответствии со сроком действия ключей. Администратор безопасности не позднее, чем за месяц до плановой смены ключей, извещает отдел эксплуатации о предстоящей плановой смене ключей. Смена ключей производится в соответствии с требованиями документации СКЗИ, и внутренним регламентом

эксплуатирующей организации или регламентом обслуживающей организации.

2.3.3 Этап передачи и установки

Распространение СКЗИ, интеграция СКЗИ в ПУ, УСПД и ИВК на производстве

Все полученные, используемые, хранимые или передаваемые СКЗИ, документация к ним должны закрепляться за ответственными лицами. Ведение непосредственных операций по учету СКЗИ, эксплуатационной и технической документации к ним в соответствии с функциональными обязанностями и инструкциями возлагается на Администратора безопасности или лицо с соответствующими функциональными обязанностями. Формуляр СКЗИ может распространяться на партию изделий, соответственно он подлежит снятию с регистрации и утилизации после снятия с учета всех перечисленных в нем изделий.

СКЗИ предусматривают встраивание в ИВК, ПУ и УСПД. Для каждой модели компонента ИСУЭ должна производиться оценка влияния компонента ИСУЭ на выполнение требований, предъявляемых к СКЗИ.

2.3.4 Этап эксплуатации

При штатной эксплуатации СКЗИ работает в автоматическом режиме.

2.3.5 Этап технического обслуживания

В случае выявления неисправности в работе СКЗИ, обслуживающий персонал обязан сообщить о данном факте Администратору безопасности. Для восстановления работоспособности СКЗИ Администратор безопасности производит переинициализацию СКЗИ. Если СКЗИ не подлежит восстановлению путём переинициализации, выдается новое инициализированное СКЗИ с оформлением записи в журнале.

При наступлении события, относящегося к компрометации ключей, персонал должен немедленно остановить работу скомпрометированного экземпляра СКЗИ и поставить в известность Администратора безопасности. По факту компрометации Администратор безопасности, действуя в соответствии с требованиями эксплуатационной документации на АРМ, производит переинициализацию СКЗИ, если это возможно, иначе выдаёт персоналу новое инициализированное СКЗИ.

Под компрометацией ключей понимаются следующие события:

- утрата устройства;
- установление факта несанкционированного доступа к СКЗИ.

При компрометации ключей следует немедленно прекратить эксплуатацию скомпрометированного устройства и поставить в известность Администратора безопасности.

По факту компрометации должно быть проведено служебное расследование с участием Администратора безопасности или специально сформированной комиссии, в рамках которого должна быть определена совокупность изделий, содержащих криптографические ключи, на которые распространяется компрометация.

После проведения служебного расследования выполняется уничтожение ключей путем уничтожения устройства или путем его переинициализации. Сертификаты, выданные на скомпрометированные ключи, должны быть отозваны.

2.3.6 Этап утилизации/вывода из эксплуатации

При выводе из эксплуатации СКЗИ происходят следующие действия:

- отключение и демонтаж устройства из компонента ИСУЭ;
- доставка устройства к (П)ЭВМ, на котором развернут АРМ инициализации;
- перепрошивка устройства в соответствии с эксплуатационной документацией на АРМ;
- передача на хранение как неиспользуемое устройство в соответствии с эксплуатационной документацией на АРМ.

3 МОДЕЛЬ НАРУШИТЕЛЯ ИБ УСПД, ПУ, ИВК, СКЗИ УСПД, СКЗИ ПУ И СКЗИ ИВК

По признаку принадлежности все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование.

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

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи. К внешним нарушителям могут относиться:

- физическое лицо (хакер);
- конкурирующие организации;
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- бывшие работники (пользователи).

Возможности **внутреннего нарушителя** существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы;
- администраторы конкретных подсистем или баз данных;
- пользователи;
- пользователи, являющиеся внешними по отношению к конкретной АС;
- лица, обладающие возможностью доступа к системе передачи данных;
- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы, но не имеющие права доступа к ним;
- обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.);
- уполномоченный персонал разработчиков, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов изделия.

3.1 Внешний нарушитель ПУ и СКЗИ ПУ

Данная модель внешнего нарушителя предполагает, что нарушитель имеет возможности к:

3.1.1 созданию способов, подготовке и проведению атак без привлечения специалистов в области разработки и анализа СКЗИ;

3.1.2 проведению атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения (для ПУ, размещаемых не на жилых зданиях).

Для ПУ, размещаемых в подъездах жилых зданий, границей контролируемой зоны является корпус ПУ.

3.1.3 проведению атак на этапе эксплуатации СКЗИ на:

- ключевую, аутентифицирующую и парольную информацию СКЗИ;
- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;
- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;

– иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и программного обеспечения (далее – ПО).

3.1.4 получению из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

- сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

- содержание находящейся в свободном доступе конструкторской документации на СКЗИ;

- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

– сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.

3.1.5 применению:

– находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

– специально разработанных АС и ПО.

3.1.6 использованию на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

– каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

– каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.

3.1.7 проведению на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

3.1.8 использованию на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

3.1.9 перехвату:

– всех данных, передаваемых по цепям средства регистрации и поступающих из СКЗИ;

– всех данных, передаваемых по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

– сигналов в каналах связи, сопровождающих функционирование одного СКЗИ.

3.1.10 осуществлению активного воздействия на СКЗИ с использованием устройств, имитирующих функционирование средства регистрации информации.

3.1.11 применению методов, основанных на наблюдении ответных реакций СКЗИ на активное воздействие.

3.1.12 применению методов инженерного проникновения.

3.2 Внутренний нарушитель ПУ и СКЗИ ПУ

Данная модель внутреннего нарушителя предполагает, что нарушитель имеет возможности к:

3.2.1 созданию способов, подготовке и проведению атак на различных этапах жизненного цикла СКЗИ.

К этапам жизненного цикла СКЗИ относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация, утилизация.

3.2.2 проведению на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.

3.3 Внешний нарушитель УСПД и СКЗИ УСПД

Данная модель внешнего нарушителя предполагает, что нарушитель имеет возможности к:

3.3.1 созданию способов, подготовке и проведению атак без привлечения специалистов в области разработки и анализа СКЗИ;

3.3.2 проведению атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения, шкафа для хранения УСПД, а также корпус УСПД.

3.3.3 проведению атак на этапе эксплуатации СКЗИ на:

- ключевую, аутентифицирующую и парольную информацию СКЗИ;
- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;
- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;
- иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и программного обеспечения (далее – ПО).

3.3.4 получению из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
- сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

- содержание находящейся в свободном доступе конструкторской документации на СКЗИ;
- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;
- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;
- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;
- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;
- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;
- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.

3.3.5 применению:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
- специально разработанных АС и ПО.

3.3.6 использованию на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

- каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;
- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.

3.3.7 проведению на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным

кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

3.3.8 использованию на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

3.3.9 физическому доступу к СВТ, на которых реализованы СКЗИ и СФ.

3.3.10 использованию штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

3.4 Внутренний нарушитель УСПД и СКЗИ УСПД

Данная модель внутреннего нарушителя предполагает, что нарушитель имеет возможности к:

3.4.1 созданию способов, подготовке и проведению атак на различных этапах жизненного цикла СКЗИ.

К этапам жизненного цикла СКЗИ относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация, утилизация.

3.4.2 проведению на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.

3.4.3 проведению атак на этапе эксплуатации СКЗИ на следующие объекты:

- документацию на СКЗИ и компоненты СФ;
- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных

функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.

3.4.4 доступу к аппаратным компонентам СКЗИ и СФ, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

3.4.5 проведению атаки при нахождении в пределах контролируемой зоны.

3.4.6 получению в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;
- сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

3.5 Внешний нарушитель ИВК и СКЗИ ИВК

Данная модель внешнего нарушителя предполагает, что нарушитель имеет возможности к:

3.5.1 созданию способов, подготовке и проведению атак без привлечения специалистов в области разработки и анализа СКЗИ;

3.5.2 проведению атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

3.5.3 проведению атак на этапе эксплуатации СКЗИ на:

- ключевую, аутентифицирующую и парольную информацию СКЗИ;
- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;
- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;

– иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и программного обеспечения (далее – ПО).

3.5.4 получению из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

– общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

– сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

– содержание находящейся в свободном доступе конструкторской документации на СКЗИ;

– содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

– общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

– сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

– все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

– сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

– сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.

3.5.5 применению:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
- специально разработанных АС и ПО.

3.5.6 использованию на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

- каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;
- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.

3.5.7 проведению на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

3.5.8 использованию на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

3.5.9 физическому доступу к СВТ, на которых реализованы СКЗИ и СФ.

3.5.10 использованию штатных средств, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

3.6 Внутренний нарушитель ИВК и СКЗИ ИВК

Данная модель внутреннего нарушителя предполагает, что нарушитель имеет возможности к:

3.6.1 созданию способов, подготовке и проведению атак на различных этапах жизненного цикла СКЗИ.

К этапам жизненного цикла СКЗИ относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация.

3.6.2 проведению на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.

3.6.3 проведению атак на этапе эксплуатации СКЗИ на следующие объекты:

- документацию на СКЗИ и компоненты СФ;
- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.

3.6.4 доступу к аппаратным компонентам СКЗИ и СФ, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

3.6.5 проведению атаки при нахождении в пределах контролируемой зоны.

3.6.6 получению в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;
- сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

4 МОДЕЛЬ УГРОЗ ИБ УСПД И ПУ

4.1 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК

4.1.1 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе производства

- Ошибка проектирования;
- Дефект, брак и НДВ.

4.1.2 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе передачи

- НСД и вскрытие;
- Несанкционированная модернизация;
- Подмена и фальсификация.

4.1.3 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе ввода в эксплуатацию

- Несанкционированная модернизация;
- Компрометация КИ.

4.1.4 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе эксплуатации

- Несанкционированная эксплуатация путем физического вмешательства;
- Компрометация КИ;
- Перехват информационных объектов, нарушение целостности сети между ИВК и УСПД, между ИВК и ПУ, между УСПД и ПУ;
- Восстановление применяемой ключевой информации;
- MITM атака между ИВК и УСПД;
- Сетевое вторжение, НСД к ПУ и УСПД;
- Внедрение ВПО в ПУ и УСПД;
- Перехват управления между ИВК и ПУ, ИВК и УСПД;
- Перехват управления средств, сопутствующих СКЗИ ПУ и СКЗИ УСПД;
- Атаки на инфраструктуру энергопотребления.

4.1.5 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе технического обслуживания и ремонта

- Несанкционированная модернизация;

- Компрометация КИ.

4.1.6 Состав и описание угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК на этапе утилизации

- Несанкционированная модернизация;
- Компрометация КИ.

4.2 Классификация угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК

№	Угроза	Объект	Канал	Ущерб
1.	Ошибка проектирования	ПУ, УСПД, ИВК	НСД	Низкий
2.	Дефект, брак и НДВ	ПУ, УСПД, ИВК	НСД	Низкий
3.	НСД и вскрытие	ПУ, УСПД, ИВК	НСД	Низкий
4.	Несанкционированная модернизация	ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	НСД, технический	Низкий
5.	Подмена и фальсификация	ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	НСД, технический	Низкий
6.	Компрометация КИ.	СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	технический	Средний
7.	Перехват информационных объектов, нарушение целостности сети между ИВК и УСПД, между УСПД и ПУ	УСПД, ИВК	технический	Средний
		ПУ, УСПД		Низкий
8.	Восстановление применяемой ключевой информации	СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	технический	Средний
9.	MITM атака между ИВК и УСПД	УСПД, СКЗИ УСПД, ИВК, СКЗИ ИВК	технический	Средний
10.	Сетевое вторжение, НСД к ПУ, УСПД и ИВК	ИВК, УСПД, СКЗИ УСПД, СКЗИ ИВК	НСД, технический	Средний
		ПУ, СКЗИ ПУ,		Низкий
11.	Внедрение ВПО в ПУ, УСПД и ИВК	УСПД, ИВК	НСД, технический	Средний
		ПУ		Низкий
12.	Перехват управления между ИВК и ПУ, ИВК и УСПД	ИВК, УСПД, СКЗИ УСПД, СКЗИ ИВК	НСД, технический	Средний
		ПУ, СКЗИ ПУ		Низкий

№	Угроза	Объект	Канал	Ущерб
13.	Перехват управления средств, сопутствующих СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	ИВК, СКЗИ ИВК УСПД, СКЗИ УСПД	НСД, технический	Средний
		ПУ, СКЗИ ПУ		Низкий
14.	Атаки на инфраструктуру энергопотребления	ИВК, УСПД, ПУ	НСД, технический	Высокий

4.3 Описание мер противодействия угрозам ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК и оценка эффективности мер противодействия угрозам ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК

№	Угроза	Риск	Тип меры защиты	Объект	Механизм защиты	Остаточный риск
1.	Ошибка проектирования	Низкий	организационно-технический	ИВК, УСПД, ПУ	Внедрение системы менеджмента качества на предприятии-производителе в т.ч. периодическая проверка соблюдения требований.	Низкий
2.	Дефект, брак и НДВ	Низкий	организационно-технический	ИВК, УСПД, ПУ	Внедрение системы менеджмента качества на предприятии-производителе в т.ч. периодическая проверка соблюдения требований.	Низкий
3.	НСД и вскрытие	Низкий	организационно-технический	ПУ, УСПД, ИВК	Введение контрольно-пропускного режима Осуществление разграничение и контроль доступа защищаемым ресурсам Оснащение помещений, в которых располагается УСПД и ИВК, входными дверями с замками, обеспечение постоянного закрытия дверей помещений на замок и открытия только для санкционированного прохода Оборудование УСПД и ИВК датчиком вскрытия	Низкий
4.	Несанкционированная модернизация	Низкий	организационно-технический	ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	Введение контрольно-пропускного режима Осуществление разграничение и контроль доступа защищаемым ресурсам Оборудование УСПД и ИВК датчиком вскрытия	Низкий

№	Угроза	Риск	Тип меры защиты	Объект	Механизм защиты	Остаточный риск
5.	Подмена и фальсификация	Низкий	организационно-технический	ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	Введение контрольно-пропускного режима Осуществление разграничение и контроль доступа защищаемым ресурсам Оборудование УСПД и ИВК датчиком вскрытия	Низкий
6.	Компрометация КИ.	Средний	технический	СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	Применение инженерно-криптографических механизмов СКЗИ и технических решений, направленных на снижение вероятности возникновения опасного события утечки КИ в канал связи	Низкий
7.	Перехват информационных объектов, нарушение целостности сети между ИВК и УСПД, между УСПД и ПУ	Средний	технический	ИВК и УСПД	Внедрение защиты каналов передачи данных с применением алгоритмов криптографических преобразований	Низкий
		Низкий		УСПД и ПУ	См. Примечание к п.7	
8.	Восстановление применяемой ключевой информации	Средний	технический	СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК	Применение усложненной схемы генерации КИ с применением датчика случайных чисел	Низкий
9.	MITM атака между ИВК и УСПД	Средний	организационно-технический	УСПД, СКЗИ УСПД, ИВК, СКЗИ ИВК	Внедрение защиты каналов передачи данных с применением алгоритмов криптографических преобразований	Низкий
10.	Сетевое вторжение, НСД к ПУ, УСПД и ИВК	Средний	технический	ИВК, УСПД, СКЗИ УСПД, СКЗИ ИВК	Внедрение СЗИ от НСД	Низкий
		Низкий		ПУ, СКЗИ ПУ		

№	Угроза	Риск	Тип меры защиты	Объект	Механизм защиты	Остаточный риск
11.	Внедрение ВПО в ПУ, УСПД и ИВК	Средний	организационно-технический	УСПД, ИВК	Введение контрольно-пропускного режима Осуществление разграничение и контроль доступа защищаемым ресурсам Оснащение помещений, в которых располагается УСПД и ИВК, входными дверями с замками, обеспечение постоянного закрытия дверей помещений на замок и открытия только для санкционированного прохода Обновление ПО ПУ, ПО УСПД, ПО ИВК только из доверенных источников	Низкий
		Низкий		ПУ		
12.	Перехват управления между ИВК и ПУ, ИВК и УСПД	Средний	организационно-технический	ИВК, УСПД, СКЗИ УСПД, СКЗИ ИВК	Введение контрольно-пропускного режима Осуществление разграничение и контроль доступа защищаемым ресурсам Оснащение помещений, в которых располагается ИВК и УСПД, входными дверями с замками, обеспечение постоянного закрытия дверей помещений на замок и открытия только для санкционированного прохода Внедрение защиты каналов передачи данных с применением алгоритмов криптографических преобразований	Низкий
		Низкий		ПУ, СКЗИ ПУ		
13.	Перехват управления средств, сопутствующих СКЗИ ПУ, СКЗИ УСПД и СКЗИ ИВК	Средний	организационно-технический	ИВК, УСПД, СКЗИ УСПД, СКЗИ ИВК	Введение контрольно-пропускного режима на предприятии изготовителе Осуществление разграничение и контроль доступа защищаемым ресурсам Оснащение помещений, в которых располагается ИВК и УСПД, входными дверями с замками, обеспечение постоянного закрытия дверей помещений на замок и открытия только для санкционированного прохода Внедрение СЗИ от НСД-	Низкий
		Низкий		ПУ, СКЗИ ПУ		
14.	Атаки на инфраструктуру энергопотребления	Высокий	организационно-технический	ИВК, УСПД, ПУ	Внедрение защиты каналов передачи данных с применением алгоритмов криптографических преобразований	Низкий

Примечание к п.7

Каналы связи между УСПД и ПУ не пролегают в сети интернет (пролегают в локальной сети объекта, где установлен УСПД). По причине необходимости физического доступа к каждому такому объекту для проведения атаки риск изначально низкий, соответственно механизм защиты в виде «Внедрение защиты каналов передачи данных с применением алгоритмов криптографических преобразований» не требуется.

Примечание к п.14

Атака на инфраструктуру энергопотребления может осуществляться путем перехвата команды управления между ИВК и УСПД и между ИВК и ПУ (размещаемых на объектах КИИ). Каналы передачи указанных команд управления защищаются с помощью внедрения защиты каналов передачи данных с применением алгоритмов криптографических преобразований

ИВК располагаются в выделенных помещениях, доступ к которым обеспечивается в соответствии с контрольно-пропускным режимом. Представители технических служб при работе в помещениях находятся только в присутствии сотрудников по эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей.

Примечание – Организация, ответственная за ввод в эксплуатацию и техническое обслуживание ПУ и УСПД, должна регламентировать сроки и порядок выездного обслуживания ПУ и УСПД, целостность которых была нарушена, вывода из эксплуатации и направление таких ПУ и УСПД на ремонтные работы.

Для ПУ и УСПД организация, ответственная за их ввод в эксплуатацию и техническое обслуживание, должна обеспечить процедуру периодического (не реже одного раза в четыре года с момента ввода ПУ/УСПД в эксплуатацию) выездного контроля целостности корпуса ПУ/УСПД и отсутствия внешних признаков, указывающих на наличие возможности физического доступа к внутренней элементной базе ПУ/УСПД. В случае наличия подобных признаков необходимо произвести вывод ПУ/УСПД из эксплуатации и направить их на ремонтные работы.

4.4 Уточнение предположения об актуальных нарушителях

В соответствии с моделью нарушителей, описанной в разделе 5 настоящего документа для ИСУЭ вероятны как внутренние, так и внешние нарушители, в связи с чем для ИСУЭ возможны атаки, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных в пункте 6.1 настоящего документа.

5 ЗАКЛЮЧЕНИЕ ОБ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК

Применение ПУ, УСПД и ИВК, разработанные с учетом требований, установленных правительством РФ для ИСУЭ, порождает как новые угрозы, так и новые возможности комплексной защиты ПУ, УСПД и ИВК в составе системы.

Целостность и аутентичность всего комплекса ПО, составляющего среду функционирования СКЗИ ПУ, УСПД и ИВК будет контролироваться с использованием централизованных доверенных серверов ИСУЭ. На этапах производства, ввода в эксплуатацию, ремонта ПУ и УСПД будет исключена загрузка недоверенного ПО.

Все значимые технологические операции прошивки ПО СКЗИ, критичных данных и транспортных секретов будут выполняться при помощи специализированных АРМ, работающих под управлением доверенных серверов ИСУЭ и сертифицированных ФСБ как СКЗИ, устойчивые к атакам со стороны пользователя.

Анализ угроз ИБ ИВК, УСПД, ПУ, СКЗИ ПУ, СКЗИ УСПД, СКЗИ ИВК показывает, что внутренний нарушитель, обеспечивающий производство, ввод в эксплуатацию, техническое обслуживание и ремонт ПУ, УСПД и ИВК будет существенно ограничен в возможностях атаки на СКЗИ и УСПД в случае, если:

- Идентификация ПУ, УСПД и ИВК в течение всего жизненного цикла будет осуществляться при помощи уникальных идентификаторов микроконтроллеров, применяемых в этих устройствах;

- Контроль подлинности экземпляра ПУ, УСПД и ИВК будет выполняться при помощи дополнительных некриптографических (транспортных) секретов, формируемых в защищенных технологических процессах и исключающие возможность подмены изделия;

- В составе ИСУЭ эксплуатируются информационные активы, существенно различающиеся по ценности и по уровню ущерба: (без учета мер по нейтрализации угроз):

- риск нарушения конфиденциальности показаний ПУ мал;
- нарушение целостности сети, потеря показаний или даже полного потока показаний ИСУЭ - малый риск;
- риски НСД к управлению энергопотреблением высокие;
- риски вмешательства в процесс конфигурирования ПУ, УСПД и ИВК не касающихся управления энергопотребления представляются низкими или средними;

- наивысшим следует признать риск реализации угроз, выполняемых по типу инфраструктурных атак, связанных с массовыми нарушениями процесса энергоснабжения потребителей.

– Анализ Методов показал, что:

- угрозами являются атаки, выполняющиеся по техническим каналам связи, и атаки НСД;
- процесс вскрытия защищенного корпуса устройства или металлического шкафа, представляющих собой периметр КЗ ПУ, УСПД, СКЗИ ПУ, СКЗИ УСПД следует признать трудоемким, требует применения инструментальных средств; выполняется в течение достаточно длительного времени, оставляет следы взлома и по всем перечисленным причинам связан с рисками обнаружения взломщика как средствами информационных систем, так и средствами физической защиты приборов и устройств, внешними средствами охраны и непосредственно гражданами, потребителями электроэнергии, не заинтересованными в нарушениях процесса их электроснабжения.

Таким образом, методом противодействия практически единственной атаки на ИСУЭ, имеющей катастрофически тяжелые последствия, является обеспечение надежной защиты ПУ, УСПД и ИВК при помощи СКЗИ от атак по техническим каналам связи.

Каналы связи между компонентами ИСУЭ не являются широкоэмиттерными, а направлены на конкретный узел. Таким образом, при перехвате сигнала ИВК массовое отключение электроэнергии не представляется возможным. В связи с этим, нарушители, соответствующие классам КА и КВ, а именно – спецслужбы иностранных государств, террористические организации и криминальные группировки, заинтересованные в нанесении ущерба государству или коммерческим структурам, не являются актуальными.

При этом реализация сетевой защиты ПУ, УСПД и ИВК может быть реализована программными или программно-аппаратными СКЗИ.

Учитывая выводы данной модели угроз, СКЗИ ПУ должны соответствовать требованиям к СКЗИ класса КС1, СКЗИ УСПД должны соответствовать требованиям к СКЗИ класса КС3, СКЗИ ИВК должны соответствовать требованиям к СКЗИ класса КС3.