УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ
Аналитический центр

АНАЛИТИЧЕСКАЯ ЗАПИСКА

Обзор приказа Минэнерго «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования»

Аналитик К.Е. Полежаев
Помощник аналитика А.А. Заведенская

2019

г. Екатеринбург

Оглавление

Список использованных сокращений

АРМ	–	Автоматизированное рабочее место
АСУТП	–	Автоматизированная система управления технологическим процессом
БДУ	–	Банк данных угроз
ИБ	–	Информационная безопасность
МЭ	–	Межсетевой экран
НДВ	–	Недокументированные (недекларированные) возможности
ПО	–	Программное обеспечение
СрЗИ	–	Средства защиты информации
СУМиД	–	Система удаленного мониторинга и диагностики основного технологического оборудования
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации

Введение

Настоящая Аналитическая записка содержит обзор опубликованного на официальном интернет-портале правовой информации 18 февраля 2019 года Приказа Министерства энергетики Российской Федерации от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования» (Зарегистрирован 15.02.2019 № 53815) (далее – Приказ Минэнерго). Приказ вступает в силу по истечении шести месяцев со дня его официального опубликования, т.е. с 18 августа 2019 года.

В сфере электроэнергетики в технологических процессах производства и передачи электроэнергии и тепла активно применяются автоматизированные системы управления технологическими процессами (далее – АСУТП). АСУТП могут интегрироваться с системами удаленного мониторинга и диагностики (далее – СУМиД) технического состояния основного оборудования объектов электроэнергетики, что требует принятия мер по обеспечению безопасности данных систем. Приказом устанавливаются организационные и функциональные требования к обеспечению информационной безопасности СУМиД, а именно безопасности ее программных компонентов, аппаратной инфраструктуры, встроенных средств защиты информации и обеспечению контроля безопасности. Также устанавливаются требования к обеспечению ИБ СУМиД на стадиях жизненного цикла и проведению аттестации.

1. Общие положения

Система удаленного мониторинга и диагностики (СУМиД) – это программно-аппаратный комплекс, обеспечивающий процесс удаленного наблюдения и контроля за состоянием основного технологического оборудования объекта электроэнергетики, диагностирование и прогнозирование изменения технического состояния основного технологического оборудования на основе собранных данных, получаемых от систем сбора данных, установленных на технологическом оборудовании, и не влияющего на штатный режим оборудования/объекта. К примеру, под указанный тип систем могут попадать: система мониторинга и диагностики «Система контроля и управления трансформаторным оборудованием» компании ЗАО «Интера», программное обеспечение от General Electric «On-Site Monitor» (OSM).

Требования Приказа Минэнерго устанавливаются в отношении **базовых функций** СУМиД и **информационной безопасности** объектов электроэнергетики при **создании** и последующей **эксплуатации** СУМиД на территории Российской Федерации. Можно сделать вывод о том, что требования распространяются на Субъекты электроэнергетики, которые эксплуатируют на объектах электроэнергетики СУМиД. В силу того, что требования по информационной безопасности предъявляются к стадии создания СУМиД, закономерно, что Субъекты электроэнергетики, использующие СУМиД сторонней разработки, будут стараться возложить выполнение части требований Приказа Минэнерго на организации, осуществляющие разработку СУМиД.

Субъектами электроэнергетики являются лица, осуществляющие деятельность в сфере электроэнергетики, в том числе производство электрической, тепловой энергии и мощности, приобретение и продажу электрической энергии и мощности, энергоснабжение потребителей, оказание услуг по передаче электрической энергии, оперативно-диспетчерскому управлению в

электроэнергетике, сбыт электрической энергии (мощности), организацию купли-продажи электрической энергии и мощности[1].

Объекты электроэнергетики – имущественные объекты, непосредственно используемые в процессе производства, передачи электрической энергии, оперативно-диспетчерского управления в электроэнергетике и сбыта электрической энергии, в том числе объекты электросетевого хозяйства. Под объектами в Приказе Минэнерго имеются в виду те объекты, на площадках которых функционирует определенное **основное технологическое оборудование,** с установленными на этом оборудовании СУМиД, имеющими определенные базовые функции.

Основное технологическое оборудование – это оборудование, нарушение или прекращение функционирования которого приводит к потере управления объектом электроэнергетики, необратимому негативному изменению параметров его функционирования, или существенному снижению безопасности эксплуатации объекта электроэнергетики.

К основному технологическому оборудованию, согласно Приказу Минэнерго относятся:

- паровые турбины, установленной мощностью 5 МВт и более и сопутствующее вспомогательное оборудование, участвующее в основном технологическом процессе, но не осуществляющее производство или преобразование электрической энергии), предназначенное для обеспечения работоспособности основного технологического оборудования (далее – вспомогательное оборудование);
- паровые (энергетические) котлы, обеспечивающие паром паровые турбины установленной мощностью 5 МВт и более, и сопутствующее вспомогательное оборудование;
- гидротурбины, установленной мощностью 5 МВт и более и сопутствующее вспомогательное оборудование;
- газовые турбины единичной мощностью более 25 МВт и сопутствующее вспомогательное оборудование;
- силовые трансформаторы напряжением 110 кВ и выше, мощностью более 63 МВА и сопутствующее вспомогательное оборудование.

2. Базовые функции и основные компоненты СУМиД

Приказом Минэнерго определены **основные** (базовые) **функции** СУМиД:

- технологический мониторинг состояния основного технологического оборудования;
- удаленное управление основным технологическим оборудованием с возможностью удаленного воздействия на основное технологическое оборудование с целью изменения параметров его функционирования или его отключения, с использованием специального программного обеспечения и (или) модуля программного обеспечения СУМиД.

На основании формулировки из Приказа Минэнерго остается неясным, следует ли относить к СУМиД систему, не осуществляющую удаленное управление основным технологическим оборудованием. Специалистами ООО «УЦСБ» был отправлен запрос в адрес Минэнерго России о разъяснения вопроса о базовых функциях СУМиД. В ответе на запрос Минэнерго России разъясняет, что требования Приказа Минэнерго распространяются как на системы осуществляющие только

[1] Согласно Федеральному закону от 26.03.2003 N 35-ФЗ «Об электроэнергетике»

технологический мониторинг, так и на системы, реализующие мониторинг и удаленное управление основным технологическим оборудованием.

В таблице 1 приведены **программные и аппаратные компоненты**, которые могут входить в состав СУМиД, согласно Приказу Минэнерго.

Таблица 1. Компоненты программного и аппаратного обеспечения СУМиД

Вид компонента	Уровень компонента	Наименование компонента
Аппаратное обеспечение	Верхний уровень	• сервер обработки информации; • маршрутизатор; • межсетевой экран; • источник бесперебойного питания; • автоматизированные рабочие места персонала
	Средний уровень	• сервер приложений; • сервер базы данных; • маршрутизатор; • межсетевой экран; • источник бесперебойного питания; • автоматизированные рабочие места (в случае привлечения организаций, предоставляющих услуги удаленного мониторинга и диагностики энергетического оборудования)
	Нижний уровень	• сервер приложений; • сервер базы данных; • маршрутизатор; • межсетевой экран; • источник бесперебойного питания; • автоматизированные рабочие места персонала
Программное обеспечение (ПО)	Верхний уровень	• ПО серверов хранения данных; • ПО обеспечения центрального сервера хранения данных; • интерфейсы автоматизированных рабочих мест персонала; • ПО для формирования, поддержания в актуальном состоянии и уточнения математических моделей СУМиД; • ПО для моделирования процессов функционирования основного технологического оборудования, построения статистических моделей для нужд мониторинга, обнаружения и локализации отклонений, определения вероятных мест возникновения аварийных ситуаций; • ПО обработки архивных данных; • ПО для расширения функциональных возможностей (дополнительные экспертные модули); • ПО для синхронизации данных
	Средний уровень	• прикладное ПО сервера хранения данных; • системное ПО сервера хранения данных; • интерфейсы автоматизированных рабочих мест персонала (интерфейсы автоматизированных рабочих мест для разработки и поддержания в актуальном состоянии математических моделей применяются для компаний, предоставляющих услугу удаленного мониторинга и диагностики основного технологического оборудования); • программное обеспечение для синхронизации данных между уровнями СУМиД.
	Нижний уровень	• прикладное ПО сервера оперативного хранения данных; • системное программное обеспечение сервера оперативного хранения данных.

Согласно Приказу Минэнерго, Субъектом электроэнергетики могут использоваться в СУМиД неполный набор программных и аппаратных компонентов из приведенного выше перечня. Также Субъектом электроэнергетики могут использоваться иные программные и аппаратные компоненты. Однако программный и аппаратный состав СУМиД должен быть утвержден Субъектом электроэнергетики в форме перечня оборудования и ПО, разрешенного к использованию.

3. Организационные требования к обеспечению ИБ СУМиД

В рамках организационных требований устанавливаются меры к организации обеспечения информационной безопасности Субъектом электроэнергетики, а также необходимые для такой организации первичные мероприятия. Минэнерго России разъясняет, что Субъект электроэнергетики может транслировать требования Приказа Минэнерго организациям, участвующим в реализации этапов жизненного цикла СУМиД посредством внесения мер и мероприятий по обеспечению информационной безопасности в Техническое задание.

Доступ персонала к ПО СУМиД должен быть реализован через процедуры идентификации и аутентификации. Для входа в учетную запись пользователя должна быть утверждена и настроена **политика паролей,** соответствующая минимальным требованиям, приведенным в таблице 2.

Таблица 2. Требования к политике паролей

Требование	Конфигурация
Минимальная длинна пароля	Не менее десяти символов
Обновление паролей	При генерации временных паролей для единовременного входа обновление не требуется. При генерации постоянного пароля доступа обновление должно осуществляться не менее одного раза в квартал
Использование символов	При формировании пароля необходимо использовать числовые, буквенные (латиница и/или кириллица, прописные и/или строчные) и специальные символы

Для доступа персонала к ПО СУМиД Субъектом электроэнергетики должны быть предусмотрены правила разграничения доступа, соответствующие следующим минимальным требованиям:

- для персонала системы в отношении СУМиД должны быть созданы учетные записи, соответствующие требованиям политики паролей;
- настройки учетных записей персонала в отношении СУМиД должны быть утверждены Субъектом электроэнергетики;
- встроенные учетные записи (неперсонифицированные учетные записи) должны быть отключены.

Для поддержания состава аппаратной конфигурации СУМиД, Субъектом электроэнергетики должны выполняться следующие процедуры:

- обеспечение поддержки технологических процессов конечным набором программного обеспечения, перечень которого должен быть утвержден;

- обеспечение организационных и технических меры регистрации событий безопасности для всего ПО, входящего в состав СУМиД;
- определение и настройка параметров обновления (временного интервала) ПО, обеспечивающего информационную безопасность;
- организация и актуализация архива проектной и эксплуатационной документации СУМиД;
- утверждение состава оборудования аппаратного обеспечения СУМиД, а также программного обеспечения, используемого для аппаратной инфраструктуры в форме перечня оборудования и программного обеспечения, разрешенного к использованию.

Приказом Минэнерго России не установлено требование обязательного тестирования работоспособности обновлений ПО, обеспечивающего информационную безопасность. Тем не менее, уязвимость «отсутствие тестирования или упрощенное тестирование программного обеспечения» входит в состав Перечня базовых уязвимостей СУМиД, необходимых для проведения анализа уязвимостей СУМиД и построения модели угроз СУМиД (Приложение 2 к Приказу Минэнерго).

Субъектом электроэнергетики должен быть проведен ряд следующих мероприятий:

- проведена **сегментация** аппаратной инфраструктуры СУМиД с обязательным выделением минимального набора сегментов (сегмент сбора, хранения и передачи данных; сегмент эксплуатации; сегмент обслуживания; системное ПО);
- разработаны Правила определения и утверждения состава аппаратной инфраструктуры СУМиД и обеспечения контроля за аппаратной инфраструктурой СУМиД;
- в местах размещения аппаратной инфраструктуры СУМиД обеспечен и регламентирован контроль физического доступа.

После выполнения процедуры сегментации Субъект электроэнергетики должен определить процессы управления информационной безопасностью СУМиД.

Для серверного оборудования и АРМ персонала Субъекта электроэнергетики, выполняющего функции управления комплексом технических средств защиты информации, информационно-телекоммуникационной инфраструктуры СУМиД, должны быть включены **персональные** межсетевые экраны (далее – МЭ). Персональные МЭ должны обеспечивать блокировку сетевого доступа, не предусмотренного функционированием СУМиД. Также должны быть установлены пароли для доступа к ПО и актуальные средства антивирусной защиты с обновлениями.

Субъектом электроэнергетики должна проводиться проверка соответствия **встроенных** средств защиты информационной безопасности **целям информационной безопасности**, к которым относятся:

- аудит событий информационной безопасности;
- обеспечение криптографической защиты;
- дискретный доступ пользователей системы;
- контроль сетевого взаимодействия;
- передача атрибутов безопасности;
- идентификация и аутентификация;

- конфигурация безопасности;
- установление доверенных соединений;
- доступность информации.

Субъект электроэнергетики должен выполнять следующий комплекс мероприятий:

- контроль проектной документации и исходного состояния программного обеспечения;
- защита от несанкционированного доступа к информации о технических и технологических параметрах основного технологического оборудования;
- формирование и хранение отчетности указанных мероприятий.

В качестве базового набора средств контроля информационной безопасности СУМиД Субъект электроэнергетики должен выполнить следующие мероприятия:

- утвердить политику информационной безопасности;
- распределить обязанности внутри организации по обеспечению информационной безопасности;
- проводить обучение и подготовку персонала по обеспечению информационной безопасности;
- проводить обучение и подготовку персонала по поддержанию режима информационной безопасности;
- организовать процессы уведомления о случаях нарушения защиты;
- применять средства антивирусной защиты;
- обеспечивать защиту данных и проектной документации;
- осуществлять контроль соответствия, утвержденной политике информационной безопасности.

Субъектом электроэнергетики должно быть проведено категорирование СУМиД в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» согласно Постановлению Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации» и обеспечено выполнение соответствующих нормативно-правовых актов по результатам категорирования.

Категорирование СУМиД Субъектом электроэнергетики может вызвать сложности в случаях, если СУМиД не является собственностью Субъекта электроэнергетики. В большинстве случаев мониторинг и диагностика состояния технологического оборудования предоставляются Субъекту электроэнергетики в качестве услуги, а поддержку СУМиД осуществляет организация – разработчик СУМиД.

Меры по защите информации должны применяться на всех стадиях (этапах) создания СУМиД, определенных ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания». Так как Приказом Минэнерго не возлагается ответственность за обеспечение информационной безопасности, специалисты ООО «УЦСБ» считают возможным указать ответственными за обеспечение информационной безопасности на всех стадиях (этапах) создания СУМиД организации-участников каждого из этапов.

4. Требования к обеспечению ИБ СУМиД на стадиях жизненного цикла

При создании и последующей эксплуатации СУМиД функция технологического мониторинга состояния основного технологического оборудования объектов электроэнергетики, в части сбора, хранения и передачи данных (центров обработки данных), должна осуществляться посредством инфраструктуры сбора, хранения и передачи данных, **расположенной на территории Российской Федерации.** При передаче данных посредством сети связи общего пользования должны применяться средства защиты информации (далее – СрЗИ), прошедшие оценку соответствия на основании требований Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании». Оценка соответствия средств защиты информации на основании требований Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» осуществляется в форме сертификации средств защиты информации.

Следует отметить, что данное требование не распространяется на инфраструктуру обработки данных. Следовательно, функция технологического мониторинга состояния основного технологического оборудования в части обработки технологических данных может осуществляться за пределами Российской Федерации.

В случае использования специального ПО и/или модуля ПО с функцией удаленного управления в СУМиД для них должна быть проведена проверка не ниже, чем по 4 уровню контроля отсутствия НДВ.

Субъектом электроэнергетики должны быть разработаны и утверждены модель угроз и нарушителя для СУМиД. Для моделирования угроз ИБ должен применяться Банк данных угроз ФСТЭК России, а также иные доступные источники и результаты оценки вероятности реализации уязвимостей компонент СУМиД. При моделировании угроз должны быть описаны источники угроз, типовые уязвимости, объекты воздействия, деструктивные действия в отношении объектов СУМиД,

На основании сформированной модели угроз информационной безопасности СУМиД осуществляется разработка политики информационной безопасности, включающей в себя функциональные требования к информационной безопасности СУМиД.

В Приказе Минэнерго не определено понятие «функциональные требований», и не приведен базовый набор функциональных требований к информационной безопасности СУМиД, на основании которого Субъект электроэнергетики смог бы сформировать собственный набор функциональных требований. Согласно мнению специалистов ООО «УЦСБ», а также на основании Проекта Приказа Минэнерго № 1015, функциональные требования формируются на основании документа «ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» (далее – ГОСТ Р ИСО/МЭК 15408-2-2013). Функциональные требования предъявляются к объекту оценки и включают в себя функциональные классы, состоящие из функциональных семейств и компонент. Объектом оценки в контексте Приказа Минэнерго будет являться СУМиД.

К функциональным классам относятся:

- аудит безопасности;
- связь;
- криптографическая поддержка;
- защита данных пользователя;

- идентификация и аутентификация;
- управление безопасностью;
- приватность;
- защита функций безопасности объекта оценки;
- использование ресурсов;
- доступ к объекту оценки;
- доверенный маршрут/канал.

Подробное описание функциональных классов их семейств и компонентов приведено в ГОСТ Р ИСО/МЭК 15408-2-2013.

Для подтверждения соответствия СУМиД и ее подсистемы безопасности Требованиям, установленным Приказом Минэнерго, СУМиД и ее подсистемы безопасности подлежат обязательной аттестации в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11.02.2013 № 17. Ввод в действие СУМиД и ее подсистемы безопасности должен осуществляться только после получения аттестата соответствия СУМиД. Минэнерго России подтверждает, что аттестации подлежат как сервера сбора данных, установленные на производственных объектах Субъектов электроэнергетики, так и сервера обработки данных СУМиД обслуживающих организаций.

На основании этого следует сделать вывод, что СрЗИ, входящие в состав СУМиД, должны пройти сертификацию в соответствии с ФЗ от 27.12.2002 № 184-ФЗ «О техническом регулировании» (пункт 11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, установленных Приказом ФСТЭК России от 11.02.2013 № 17).

Следует заметить, что в случае размещения сегмента, осуществляющего обработку технологической информации за пределами Российской Федерации, невозможно выполнить аттестацию сегмента обработки технологической информации на соответствие Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17.

Также затрудняется использование прошедших сертификацию в соответствии с ФЗ от 27.12.2002 № 184-ФЗ «О техническом регулировании» средств криптографической защиты информации в сегменте обработки технологической информации, расположенном за пределами Российской Федерации, ввиду регулирования Центром по лицензированию, сертификации и защите государственной тайны ФСБ России ввоза на таможенную территорию Евразийского экономического союза и территорию Российской Федерации и вывоза за их пределы шифровальных (криптографических) средств.

Для обеспечения системы безопасности СУМиД, Субъектом электроэнергетики должны выполняться требования, установленные главами III, IV и V приказа ФСТЭК России от 21.12.2017 № 235.

Информационная безопасность СУМиД, являющихся значимыми объектами критической информационной инфраструктуры Российской Федерации, должна обеспечиваться Субъектом электроэнергетики в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25.12.2017 № 239 и с Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21.12.2017 №235.

Как следствие, если по результатам категорирования был сделан вывод об отсутствии необходимости присвоения СУМиД категории значимости, то требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры все равно остаются обязательными к выполнению, а именно требования к применению СрЗИ, прошедших сертификацию. Аналогично и с требованиями к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры. По этим требованиям для объектов критической информационной инфраструктуры должны быть проведены планирование и разработка мероприятий по обеспечению безопасности, реализация (внедрение) этих мероприятий, обеспечен контроль состояния безопасности и проводиться совершенствования безопасности.

Выводы

1. Рассматриваемый Приказ Минэнерго утверждает комплекс мер по обеспечению информационной безопасности СУМиД, которые влияют на функционирование основного технологического оборудования Субъектов электроэнергетики. Приказ вступает в силу 15 августа 2019 года.
2. Приказ Минэнерго относит СУМиД к объектам критической информационной инфраструктуры и предписывает проведение категорирования СУМиД согласно Постановлению Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации». Впоследствии Субъекты электроэнергетики должны реализовать требования, установленные приказом ФСТЭК России от 21.12.2017 № 235 и Приказом ФСТЭК России от 25.12.2017 № 239 для критически значимых объектов, которые хоть и имеют схожесть с требованиями Приказа, но не исключают обязанностей по их выполнению. Если в отношении СУМиД будет сделан вывод об отсутствии необходимости присвоения категории значимости, то обязательными к выполнению будут только требования Приказа Минэнерго.
3. Выполнение требований Приказа Минэнерго должно помочь в снижении рисков для критически важных объектов, которые связаны с СУМиД, в части минимизации угрозы удаленного управления объектами или нарушения целостности информации, на основе которой принимаются управленческие решения.
4. Используемые в СУМиД средства защиты информации должны пройти сертификацию в соответствии с ФЗ от 27.12.2002 № 184-ФЗ «О техническом регулировании». Относительно встроенных средств защиты информации Субъектом должна быть проведена проверка соответствия целям ИБ.
5. В Приказе Минэнерго содержится описание модели угроз для СУМиД, адаптированной для сферы электроэнергетики. В качестве входных данных для моделирования угроз используется Банк данных угроз ФСТЭК России и результаты оценки вероятности реализации уязвимостей компонентов СУМиД. Также в Приказе Минэнерго представлен перечень базовых атак на СУМиД, выполняемых при реализации угроз безопасности информации, который необходимо учитывать при анализе уязвимостей; перечень базовых уязвимостей, основные деструктивные действия и классификация для модели нарушителя.
6. В случае, если СУМиД обладает функционалом удаленного управления основным технологическим оборудованием, то для такого программного обеспечения и/или модуля

программного обеспечения СУМиД должна быть проведена проверка не ниже, чем по 4 уровню контроля отсутствия недекларированных возможностей.

7. Основными требованиями Приказ Минэнерго являются:
    - проведение аттестации СУМиД на соответствие требованиям, установленным приказом ФСТЭК России от 11.02.2013 № 17;
    - применение в СУМиД средств защиты информации, сертифицированным по требованиям Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании».