Приказ Минэнерго России 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"

Зарегистрировано в Минюсте России 15.02.2019 № 53815

В соответствии с пунктом 1 подпункта «б» постановления Правительства Российской Федерации от 02.03.2017 № 244 «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты Правительства Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 11, ст. 1562) приказываю:

Утвердить прилагаемые требования 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.

Министр
А.В.Новак

Требования 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

Утвержден
приказом Минэнерго России
от 06.11.2018 № 1015

I. Общие положения

1.1. Настоящие требования устанавливаются в отношении базовых (обязательных) функций программно-аппаратного комплекса, обеспечивающего процесс удаленного наблюдения, управления и контроля за состоянием оборудования/объекта электроэнергетики, диагностирование и прогнозирование изменения технического состояния оборудования/объекта электроэнергетики на основе собранных данных (исторические данные о состоянии оборудования) и операционных данных, получаемых от систем сбора данных, установленных на оборудовании, и не влияющего на штатный режим оборудования/объекта (далее - система удаленного мониторинга и диагностики, СУМиД), и к информационной безопасности СУМиД при ее создании и последующей эксплуатации.

1.2. Требования включают в себя организационные требования к обеспечению информационной безопасности систем удаленного мониторинга и диагностики основного технологического оборудования и требования к обеспечению информационной безопасности систем удаленного мониторинга и диагностики при их создании и последующей эксплуатации.

1.3. Субъекты электроэнергетики должны руководствоваться требованиями в отношении базовых (обязательных) функций обеспечения информационной безопасности систем удаленного мониторинга и диагностики основного технологического оборудования (далее - требования) при создании и последующей эксплуатации на объектах электроэнергетики СУМиД.

1.4. Настоящие требования распространяются на объекты электроэнергетики, на основном технологическом оборудовании (в соответствии с перечнем пункта 1.5 требований) которых используется СУМиД, базовые (обязательные) функции которой соответствуют перечню пункта 1.6 требований.

1.5. Основным технологическим оборудованием, нарушение или прекращение функционирования которого приводит к потере управления объектом электроэнергетики, его необратимому негативному изменению или разрушению или существенному снижению безопасности эксплуатации объекта электроэнергетики на длительный период времени, являются:
паровые турбины, установленной мощностью 5 МВт и более;
паровые (энергетические) котлы, обеспечивающие паром паровые турбины установленной мощностью 5 МВт и более;
гидротурбины, установленной мощностью 5 МВт и более;
газовые турбины, установленной мощностью 5 МВт и более;
силовые трансформаторы напряжением 110 кВ и выше.

1.6. Выполняемые СУМиД операции в соответствии с назначением являются базовые (обязательным) функции. Базовые функции

системы СУМиД включают в себя:

1.6.1. Технологический мониторинг состояния основного и вспомогательного энергетического оборудования, включая:
выявление на ранних стадиях изменений в техническом состоянии энергетического оборудования;
оценку остаточного ресурса элементов энергетического оборудования;
прогнозирование вероятности наступления аварийных событий;
определение локализованного перечня технологических параметров, способствующих отклонению показателей функционирования энергетического оборудования от эталонных моделей.

1.6.2. Удаленный контроль фактического технического состояния основного технологического оборудования, включая:
сбор, передачу, хранение данных о состояния энергетического оборудования объектов электроэнергетики и формирование статистики на основании математических моделей, с целью выдачи рекомендаций по техническому обслуживанию и эксплуатации оборудования объектов электроэнергетики, а также повышению надежности и долговечности их работы;
предоставление предиктивных (прогностических) уведомлений о возможных неисправностях и выдача рекомендации по их устранению/

1.6.3. Удаленное управление основным технологическим оборудованием объектов энергетики Российской Федерации, включая удаленное воздействие на основное технологическое оборудование, с целью изменения параметров его функционирования или отключение.

1.7. Для реализации базовых (обязательных) функций СУМиД состоит из следующих основных компонент:
аппаратного обеспечения первого, второго и третьего уровней;
программного обеспечения первого, второго и третьего уровней.

1.7.1. Аппаратное обеспечение СУМиД первого уровня состоит из:
сервера обработки информации;
маршрутизатора;
межсетевого экрана;
источника бесперебойного питания;
автоматизированных рабочих мест персонала, по анализу текущего состояния энергетического оборудования, обработке архивных данных и разработке математических моделей, инженеров, администраторов, обслуживающего персонала.

1.7.2. Аппаратное обеспечение СУМиД второго уровня состоит из:
сервера приложений;
сервера базы данных;
маршрутизатора;
межсетевого экрана;
источника бесперебойного питания;
автоматизированных рабочих мест обслуживающего персонала и администраторов системы, инженера, выполняющего функцию анализа текущего состояния энергетического оборудования, для разработки и поддержания в актуальном состоянии математических моделей (опционально для отдельных компаний, предоставляющих услугу удаленного мониторинга и диагностики энергетического оборудования).

1.7.3. Аппаратное обеспечение СУМиД третьего уровня состоит из:
сервера приложений;
сервера базы данных;
маршрутизатора;
межсетевого экрана;
источника бесперебойного питания;
автоматизированных рабочих мест обслуживающего персонала и администраторов системы.

1.7.4. Программное обеспечение первого уровня обеспечивает реализацию функций сбора данных с нижних уровней (второго и третьего уровней), генерацию отчетов, формирование и актуализацию математических моделей, расчет прогнозных состояний энергетического оборудования. Программное обеспечение системы СУМиД первого уровня состоит из:
прикладного программного обеспечения серверов хранения данных;
системного программного обеспечения центрального сервера хранения данных;
интерфейсов автоматизированных рабочих мест персонала по анализу текущего состояния энергетического оборудования, обработке архивных данных и разработке математических моделей, инженеров, администраторов, обслуживающего персонала;
программное обеспечение для формирования, поддержания в актуальном состоянии и уточнения математических моделей СУМиД;
программные средства для моделирования процессов энергетического оборудования, построения статистических моделей для нужд мониторинга, обнаружения и локализации отклонений, определения вероятных мест возникновения аварийных ситуаций;
программные средства обработки архивных данных;
программное обеспечения для расширения функциональных возможностей (дополнительные экспертные модули);
программные средства синхронизации данных.

1.7.6. Программное обеспечение второго уровня обеспечивает сбор данных телеметрии с третьего уровня СУМиД, накопление данных и передачу данных на первый уровень (в отдельных случаях возможна иная схема работы программного обеспечения второго уровня), генерацию запросов на первый уровень, начальный (базовый) анализ технического состояния энергетического оборудования, предварительная обработка предупредительных сообщений СУМиД, инициализация дополнительных сравнительных функций, формирование отчетов. Программное обеспечение СУМиД второго уровня состоит из:
прикладного программного обеспечения сервера хранения данных;
системного программного обеспечения сервера хранения данных;

интерфейсов автоматизированных рабочих мест обслуживающего персонала и администраторов системы, инженера, выполняющего функцию анализа текущего состояния энергетического оборудования, для разработки и поддержания в актуальном состоянии математических моделей (интерфейсы автоматизированных рабочих мест для разработки и поддержания в актуальном состояния математических моделей применяются для компаний, предоставляющих услугу удаленного мониторинга и диагностики энергетического оборудования);
программных средств синхронизации данных между уровнями СУМиД.

1.7.7. Программное обеспечение СУМиД третьего уровня обеспечивает временное хранение информации, а также последующую передачу необработанных данных на верхние уровни. Программное обеспечение СУМиД третьего уровня состоит из:
прикладного программного обеспечения сервера оперативного хранения данных;
системного программного обеспечения сервера оперативного хранения данных.

II. Организационные требования к обеспечению информационной безопасности систем удаленного мониторинга и диагностики основного технологического оборудования

2.1. Организационные требования к обеспечению информационной безопасности СУМиД основного технологического оборудования включают в себя организационные требования к обеспечению информационной безопасности:
программных компонент СУМиД;
аппаратной инфраструктуры СУМиД;
встроенных средств защиты информации;
организационные требования к обеспечению контроля информационной безопасности СУМиД.

2.2. Организационные требования к обеспечению информационной безопасности программных компонент СУМиД предназначены для формирования правил субъектом электроэнергетики по обеспечению процессов доступа к программному обеспечению СУМиД персонала, организации процессов поддержки функциональных требований СУМиД.

2.2.1. Доступ персонала к программному обеспечению СУМиД реализуется через процедуры идентификации и персонификации.

Для входа в учетную запись пользователя должна быть преднастроена политика паролей, соответствующая минимальным требованиям, приведенным в таблице № 1:

Таблица № 1

Требование	Конфигурация
Минимальная длинна пароля	Не менее десяти символов
Подтверждение паролей	Подтверждение паролей осуществляется администратором системы, после проверки на соответствие требованиям минимальной длинны паролей и использования специальных символов
Обновление паролей	При генерации временных паролей для единовременного входа обновление не требуется. При генерации пароля доступа обновление должно осуществляться на еженедельной основе
Использование символов	При формировании пароля необходимо использовать числовые, буквенные (латиница и/или кириллица, прописные и/или строчные) и специальные символы

Для доступа персонала к программному обеспечению СУМиД должна быть предусмотрена его категоризация, утвержденная субъектом электроэнергетики правилами доступа, соответствующая следующим минимальным требованиям, приведенным в таблице № 2:

Таблица № 2

Категория пользователей программного обеспечения СУМиД	Требования к организации доступа к программному обеспечению СУМиД
Администраторы системы	Для каждого администратора системы должны быть создана учетная запись, соответствующая требованиям политики паролей. Настройки учетной записи администратора системы должны быть утверждены службой информационной безопасности объекта электроэнергетики
Обслуживающий персонал и диспетчеры системы	Для каждого сотрудника обслуживающего персонала и диспетчеров системы должна быть создана учетная запись соответствующая требованиям политики паролей. Настройки учетной записи обслуживающего персонала и диспетчеров системы должны быть утверждены службой безопасности объекта
Пользователи	Для каждого пользователя создается временная учетная запись и генерируется временный пароль. Настройки учетной записи пользователей должны быть утверждены службой информационной безопасности электроэнергетики
Встроенные учетная запись (неперсонифицированные учетные записи)	Должна быть отключена

2.2.2. Поддержка функциональных требований информационной безопасности к программным компонентам СУМиД должна обеспечиваться субъектом электроэнергетики с учетом следующих требований:
поддержка технологических процессов должна обеспечиваться конечным набором программных средств, утвержденных субъектом электроэнергетики;
для всех программных средств, входящих в состав СУМиД, должны быть реализованы и включены средства регистрации событий

безопасности, а также определены в регламенте, утвержденном субъектом электроэнергетики, и настроены процедуры обновления (временной интервал) программного обеспечения для информационной безопасности.

2.2.3. Субъектом электроэнергетики должен быть организован архив проектной и эксплуатационной документации для СУМиД, доступ к которому должен быть регламентирован.

Проектная и эксплуатационная документация должна актуализироваться по утвержденному субъектом электроэнергетики регламенту.

2.3. Организационные требования к обеспечению информационной безопасности аппаратной инфраструктуры СУМиД предназначены для формирования правил определения и утверждения состава аппаратной инфраструктуры СУМиД и обеспечения процессов контроля за аппаратной инфраструктурой СУМиД субъектом электроэнергетики.

2.3.1. Состав оборудования аппаратной инфраструктуры СУМиД, включающей в себя указанные в пункте 1.7 настоящих требований компоненты, а также программного обеспечения, используемого для аппаратной инфраструктуры, должен утверждаться субъектом электроэнергетики в форме разрешенного перечня оборудования и программного обеспечения.

2.3.2. Для утверждения минимального набора сегментов аппаратной инфраструктуры СУМиД субъектов электроэнергетики должна быть осуществлена процедура определения основных составных частей СУМиД (далее - сегментация).

По результатам сегментации аппаратная инфраструктура СУМиД должна включать в себя минимальный набор сегментов, состоящий из:
сегмента сбора, хранения и передачи данных - программное и аппаратное обеспечение нижнего уровня, осуществляющее сбор данных с датчиков оборудования, межсетевые экраны, системы хранения данных;
сегмента эксплуатации - программное и аппаратное обеспечение среднего уровня, осуществляющее первичную обработку и представление данных, автоматизированные рабочие места эксплуатирующего персонала;
сегмента обслуживания - программное и аппаратное обеспечение верхнего уровня, обеспечивающее обработку и представление данных с функциями:
прогнозирования, сценарного моделирования, графического представления технического состояния оборудования, автоматизированные рабочие места эксплуатирующего персонала;
системного программного обеспечения - программное обеспечение, которое обеспечивает управление аппаратными компонентами технических средств и функционирование прикладного программного обеспечения.

2.3.3. По результатам сегментации субъектом электроэнергетики должны обеспечиваться процессы управления информационной безопасностью:
информационно-телекоммуникационной инфраструктурой СУМиД;
комплексом технических средств защиты информации;
программными и аппаратными средствами СУМиД.

2.3.4. Физический доступ персонала объекта к сегментам аппаратной инфраструктуры СУМиД должен устанавливаться правилами доступа и утверждаться субъектом электроэнергетики.

Правила доступа персонала объекта к сегментам аппаратной инфраструктуры СУМиД должны содержать минимальный набор положений, устанавливающих порядок доступа персонала в зависимости от функций управления:
информационно-телекоммуникационной инфраструктурой СУМиД;
комплексом технических средств защиты информации;
программными и аппаратными средствами СУМиД.

Персоналом, выполняющим функции управления программными и аппаратными средствами СУМиД должен по умолчанию устанавливаться запрет на использование программного обеспечения, не внесенного в списки разрешенного к использованию.

Список разрешенного к использованию программного обеспечения утверждается субъектом электроэнергетики с учетом категорий пользователей СУМиД, приведенных в таблице № 2 настоящих требований.

2.3.5. Персоналом объекта, выполняющим функции управления комплексом технических средств защиты информации, информационно-телекоммуникационной инфраструктуры СУМиД, в отношении серверного оборудования и автоматизированных рабочих мест должны быть обеспечены следующие меры информационной безопасности:
включены персональные межсетевые экраны, которые должны обеспечивать блокировку сетевого доступа, не предусмотренного функционированием СУМиД;
установлены пароли для доступа персонала к программному обеспечению, актуальные средства антивирусной защиты с обновлениями.

2.3.6. Для предотвращения угроз информационной безопасности в отношении аппаратной инфраструктуры СУМиД субъектом электроэнергетики должна обеспечиваться безопасность среды функционирования.

Для обеспечения безопасности среды функционирования СУМиД должен быть реализован минимальный комплекс мероприятий в соответствии с таблицей № 1 приложения № 1 к настоящим требованиям.

2.4. Организационные требования к обеспечению информационной безопасности встроенных средств защиты информации устанавливаются для предотвращения угроз информационной безопасности в отношении СУМиД.

2.4.1. Для обеспечения безопасности СУМиД должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки,

установленных пунктом 18 приказа ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарегистрирован Минюстом России 22.02.2018, регистрационный № 50118) (далее - приказ от 21.12.2017 № 235).

2.4.2. Для реализации организационных требований к встроенным средствам защиты информации СУМиД устанавливаются следующие цели информационной безопасности объекта электроэнергетики:
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.

Описание целей информационной безопасности приведены в таблице № 2 приложения № 1 настоящих требований.

2.4.3. Субъектом электроэнергетики в качестве мер по обеспечению предотвращения угроз информационной безопасности СУМиД должна проводиться проверка соответствия встроенных средств защиты информационной безопасности целям информационной безопасности объекта электроэнергетики.

2.5. Организационные требования к обеспечению контроля информационной безопасности СУМиД определяют процессы контроля субъектом электроэнергетики соответствия и исполнения требований информационной безопасности СУМиД.

2.5.1. Субъектом электроэнергетики должен осуществляться контроль соответствия и исполнения требований информационной безопасности СУМиД.

В целях обеспечения мер по предотвращению утечек информации, сбор, обработка и хранение которой осуществляется СУМиД, субъектом электроэнергетики должен реализовываться комплекс мероприятий:
по контролю документации и исходного состояния программного обеспечения;
по проведению статистического анализа исходных текстов программ;
по обеспечению формирования и хранения отчетности указанных мероприятий.

2.5.2. По результатам категорирования СУМиД в соответствии с правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации 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» (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204), субъектом электроэнергетики должны реализовываться:
требования к организационно-распорядительным документам по безопасности значимых объектов, в соответствии с главой IV приказа ФСТЭК России от 21.12.2017 № 235;
проверка требований к обеспечению безопасности СУМиД, установленных пунктом 11 приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован Минюстом России 26.03.2018, регистрационный № 50524).

2.5.3. В качестве базового набора средств контроля информационной безопасности субъект электроэнергетики должен:
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 защиты от исполняемых (компьютерных, программных) кодов или интерпретируемых наборов инструкций, обладающих свойством несанкционированного распространения и самовоспроизведения (далее - вирусы);
обеспечивать защиту данных и документации;
осуществлять контроль соответствия, утвержденной политике информационной безопасности.

IV. Требования к обеспечению информационной безопасности СУМиД при их создании и последующей эксплуатации

3.1. В целях обеспечения информационной безопасности СУМиД при создании и последующей эксплуатации СУМиД функция удаленного контроля фактического технического состояния основного технологического оборудования объектов электроэнергетики, в части сбора, хранения и передачи данных, должна осуществляться посредством инфраструктуры, расположенной на территории Российской Федерации, а программное обеспечение, используемое для осуществления функции удаленного управления основного технологического оборудования объектов электроэнергетики должно быть сертифицировано по требованиям контроля отсутствия недекларированных возможностей первого уровня контроля.

3.2. Требования к обеспечению информационной безопасности СУМиД включают в себя требования к профилю защиты,

функциональные требования и требования доверия.

3.2.1. Требования к профилю защиты включают в себя процедуру моделирования и базовую модель угроз информационной безопасности СУМиД.

В качестве основы для моделирования угроз информационной безопасности СУМиД используются критерии:
ценности (важности) рассматриваемой системы и ее компонентов;
существующих уязвимостей системы и ее компонентов;
вероятности их реализации (использования);
опасности рассматриваемой угрозы с точки зрения потенциальных последствий и деструктивных действий, выполняемых в результате реализации угроз.

В качестве входных данных для анализа угроз информационной безопасности используются:
банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541, 2017, № 48, ст. 7198), а также иные доступные источники, содержащие сведения об уязвимостях и угрозах безопасности информации СУМиД;
результаты оценки вероятности реализации уязвимостей компонент СУМиД.

На основании входных данных для анализа угроз информационной безопасности формируется перечень актуальных угроз информационной безопасности СУМиД.

Базовая модель угроз информационной безопасности СУМиД должна включать в себя:
описание СУМиД, с учетом пункта 1.7 настоящих требований, характеристики функций СУМиД, а также учитывать результаты процедуры сегментации;
описание источников угроз, типовых уязвимостей, объектов воздействия, деструктивных действий в отношении СУМиД;
модели нарушителя информационной безопасности СУМиД.

Основными источниками угроз информационной безопасности СУМиД являются:
конкуренты;
зарубежные спецслужбы;
криминальные элементы (структуры);
недобросовестные партнеры;
работники (персонал) организации (субъекта электроэнергетики);
злонамеренные высококвалифицированные специалисты информационных технологий, киберпреступники (хакеры);
разработчики и производители технических средств и программного обеспечения.

Типовые уязвимости СУМиД могут быть реализованы на прикладном и канальном уровне базовой модели стека сетевых протоколов (далее - модель OSI).

Анализ уязвимостей должен быть проведен:
на транспортном и сетевом уровнях классической модели OSI;
для семейства протоколов, предоставляющих интерфейс для управления объектами автоматизации и технологическими процессами;
для операционных систем.

При анализе уязвимостей необходимо использовать перечень атак, приведенный в таблице № 1 приложения № 2 к настоящим требованиям.

Перечень базовых уязвимостей СУМиД приведен в таблице № 2 приложения № 2 к настоящим требованиям.

Основными объектами воздействия СУМиД являются:
серверы автоматизированной системы управления и СУМиД второго и третьего уровней;
сетевой контур взаимодействия между:
сервером СУМиД нижнего уровня и автоматизированным рабочим местом обслуживающего персонала;
серверами СУМиД третьего, второго и первого уровней;
сервером СУМиД первого уровня и прикладным программным обеспечением (средства обработки данных и разработки математических моделей);
сервером СУМиД и автоматизированным рабочим местом диспетчеров и пользователей системы.

Основными деструктивными действиями в отношении безопасности информации СУМиД являются:
несанкционированное копирование информации (деструктивное действие 1 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
уничтожение информации (носителя информации) (деструктивное действие 2 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
модифицирование информации (изменение исходной информации на ложную) (деструктивное действие 3 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
блокирование информации (деструктивное действие 1 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
перехват информации при ее передаче по каналам связи (деструктивное действие 5 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);

разглашение информации персоналом (деструктивное действие 6 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
хищение носителя информации (деструктивное действие 7 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
нанесение ущерба здоровью персонала и окружающим людям (деструктивное действие 8 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
нанесение ущерба окружающей среде (деструктивное действие 9 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
физическое повреждение объекта защиты или его компонент (деструктивное действие 10 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям);
блокирование контроля над объектом защиты (деструктивное действие 11 в соответствии с нумерацией, приведенной в таблице № 1 приложения № 3 к настоящим требованиям).

Для определения возможных деструктивных действий для каждой из угроз информационной безопасности используется таблица № 2 приложения № 3 к настоящим требований.

Модель нарушителя информационной безопасности СУМиД устанавливается субъектом электроэнергетики для обеспечения контроля информационной безопасности компонент СУМиД, приведенных в пункте 1.7 настоящих требований и категорий пользователей.

Для установления модели нарушителя информационной безопасности СУМиД проводится его классификация по следующим основным направлениям:
по отношению к СУМиД;
по правам доступа к компонентам СУМиД;
по мотивации нарушения;
по возможностям физического доступа;
по квалификации;
по направлению реализации угроз информационной безопасности.

По итогам процедур классификации субъектом электроэнергетики должны быть утверждены типовые модели нарушителей СУМиД. Классификация для установления модели нарушителей приведена в приложении № 4 к настоящим требованиям.

3.2.2. Функциональные требования к информационной безопасности СУМиД устанавливаются субъектом электроэнергетики для достижения целей информационной безопасности. Взаимосвязь функциональных требований информационной безопасности и целей информационной безопасности представлена в таблице № 1 приложения № 5 к настоящим требованиям.

3.2.3. Для установления функциональных требований субъектом электроэнергетики используются функциональные компоненты и функциональные классы (функциональные компоненты включены в функциональные классы). Перечень функциональных компонент представлен в таблице № 2 приложения № 5 к настоящим требованиям.

Контроль достаточности функциональных требований осуществляется субъектом электроэнергетики в соответствии с таблицами №№ 3 - 9 приложения № 5 к настоящим требованиям.

3.2.4. Для подтверждения достаточности оснований соответствия СУМиД целям безопасности, устанавливаются требования доверия.

Требования доверия состоят из классов доверия и компонентов доверия (компоненты доверия включены в классы доверия). Описание взаимосвязи классов доверия с компонентами доверия и их идентификаторами представлены в таблице № 1 приложения № 6 к настоящим требованиям.

Компоненты доверия используются при создании и последующей эксплуатации СУМиД для достижения целей информационной безопасности, приведенных в приложении № 1 к настоящим требованиям. Классы доверия используются для оценки и установления уровней доверия в отношении СУМиД.

Для подтверждения соответствия установленных субъектом электроэнергетики требований доверия, субъектом электроэнергетики должна проводиться соответствующая оценка.

Основные требования к проведению оценки соответствия требований доверия, представленных в таблицах №№ 2 - 8 приложения № 6 к настоящим требованиям.

3.3. Для обеспечения системы безопасности СУМиД субъектом электроэнергетики должны устанавливаться требования ко встроенным средствам защиты.

Субъект электроэнергетики для обеспечения системы безопасности компонент СУМиД, установленных пунктом 1.7 настоящих требований, должен соответствовать требованиям, установленным главой III приказа ФСТЭК России от 21.12.2017 № 235.

Субъект электроэнергетики при организации работ по обеспечению безопасности СУМиД в рамках функционирования системы безопасности должен соответствовать требованиям, установленным главой V приказа ФСТЭК России от 21.12.2017 № 235.

Приложения

Приложения №№ 1-6 к приказу Минэнерго России от 06.11.2018 № 1015

безопасность критической информационной инфраструктуры, техническая защита информации