Министерство энергетики Российской Федерации

(Минэнерго России)

ПРИКАЗ

6 ноября 2018 г. № 1015

Москва

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

В соответствии с подпунктом «б» пункта 1 постановления Правительства Российской Федерации от 2 марта 2017 г. № 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; 2018, № 34, ст. 5483) п р и к а з ы в а ю:

1. 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.

2. Настоящий приказ вступает в силу по истечении шести месяцев со дня его официального опубликования.

Министр А.В. Новак

Департамент оперативного контроля
и управления в электроэнергетике
Медведева Елена Анатольевна
(495) 631-88-71

УТВЕРЖДЕНЫ
приказом Минэнерго России
от «06» 11 2018 г. №1015

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

I. Общие положения

1. Настоящие требования устанавливают организационные и функциональные требования к базовым (обязательным) функциям и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики основного технологического оборудования, нарушение или прекращение функционирования которого приводит к потере управления объектом электроэнергетики, необратимому негативному изменению параметров его функционирования (разрушению) или существенному снижению безопасности эксплуатации объекта электроэнергетики (далее – СУМиД, основное технологическое оборудование соответственно).

2. Для целей настоящих требований под СУМиД понимаются программно-аппаратные комплексы, обеспечивающие процесс удаленного наблюдения и контроля за состоянием основного технологического оборудования, диагностирование и прогнозирование изменения технического состояния основного технологического оборудования на основе собранных данных, получаемых от систем сбора данных, установленных на указанном технологическом оборудовании, основные функции которых приведены в пункте 4 настоящих требований.

3. Настоящие требования распространяются на объекты электроэнергетики:

а) на основном технологическом оборудовании которых функционирует СУМиД, обеспечивающие реализацию основных функций приведенных в пункте 4 настоящих требований;

б) основное технологическое оборудование которых соответствует следующим видам и параметрам:

паровые турбины установленной мощностью 5 МВт и более и сопутствующее оборудование, участвующее в основном технологическом процессе, но не осуществляющее производство или преобразование электрической энергии (далее – вспомогательное оборудование) и предназначенное для обеспечения работоспособности паровых турбин;

паровые (энергетические) котлы, обеспечивающие паром паровые турбины установленной мощностью 5 МВт и более, и сопутствующее вспомогательное оборудование, предназначенное для обеспечения работоспособности паровых (энергетических) котлов;

гидротурбины установленной мощностью 5 МВт и более и сопутствующее вспомогательное оборудование, предназначенное для обеспечения работоспособности гидротурбин;

газовые турбины единичной мощностью более 25 МВт и сопутствующее вспомогательное оборудование, предназначенное для обеспечения работоспособности газовых турбин;

силовые трансформаторы напряжением 110 кВ и выше мощностью более 63 МВА и сопутствующее вспомогательное оборудование, предназначенное для обеспечения работоспособности силовых трансформаторов.

4. Для выполнения организационных и функциональных требований к информационной безопасности субъект электроэнергетики при создании и последующей эксплуатации СУМиД должен руководствоваться основными функциями СУМиД, к которым относятся:

а) технологический мониторинг состояния основного технологического оборудования с:

выявлением на ранних стадиях изменений технического состояния основного технологического оборудования;

оценкой остаточного ресурса элементов основного технологического оборудования;

прогнозированием вероятности наступления аварийных событий;

определением перечня технологических параметров, характеризующих отклонение показателей функционирования основного технологического оборудования от эталонных моделей;

сбором, передачей, хранением данных о состоянии основного технологического оборудования и формированием статистики на основании математических моделей с целью повышения надёжности его работы, выдачей рекомендаций по техническому обслуживанию и эксплуатации основного технологического оборудования;

предоставлением прогностических уведомлений о возможных неисправностях основного технологического оборудования и выдачей рекомендаций по их устранению;

б) 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.

5. Субъект электроэнергетики должен соблюдать настоящие требования с учетом организационных и функциональных требований, направленных на блокирование (нейтрализацию) угроз безопасности информации, связанных с нарушением ее конфиденциальности, целостности и доступности.

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

6. Субъект электроэнергетики должен соблюдать организационные требования к обеспечению информационной безопасности СУМиД основного

технологического оборудования с учетом организационных требований к компонентам программного обеспечения СУМиД, аппаратной инфраструктуры СУМиД, встроенных средств защиты информации, обеспечению контроля информационной безопасности СУМиД.

7. В целях выполнения организационных требований к обеспечению информационной безопасности СУМиД основного технологического оборудования субъект электроэнергетики должен использовать следующие компоненты программного и аппаратного обеспечения СУМиД:

аппаратное обеспечение верхнего, среднего и нижнего уровней;

программное обеспечение верхнего, среднего и нижнего уровней.

Для аппаратного обеспечения СУМиД верхнего уровня субъект электроэнергетики должен использовать следующие компоненты:

сервер обработки информации;

маршрутизатор;

межсетевой экран;

источники бесперебойного питания;

автоматизированные рабочие места персонала.

Для аппаратного обеспечения СУМиД среднего уровня субъект электроэнергетики должен использовать следующие компоненты:

сервер приложений;

сервер базы данных;

маршрутизатор;

межсетевой экран;

источник бесперебойного питания;

автоматизированные рабочие места персонала (в случае привлечения субъектом электроэнергетики организаций, предоставляющих услуги удаленного мониторинга и диагностики энергетического оборудования).

Для аппаратного обеспечения СУМиД нижнего уровня субъект электроэнергетики должен использовать следующие компоненты:

сервер приложений;

сервер базы данных;

маршрутизатор;

межсетевой экран;

источник бесперебойного питания;

автоматизированные рабочие места персонала.

Для программного обеспечения СУМиД по реализации функций сбора данных со среднего и нижнего уровней, формирования отчетов, формирования и актуализации математических моделей, расчета прогнозных состояний энергетического оборудования (программное обеспечение верхнего уровня СУМиД) субъект электроэнергетики должен использовать следующие компоненты:

программное обеспечение серверов хранения данных;

программное обеспечение центрального сервера хранения данных;

интерфейсы автоматизированных рабочих мест персонала;

программное обеспечение для формирования, поддержания в актуальном состоянии и уточнения математических моделей СУМиД;

программное обеспечение для моделирования процессов функционирования основного технологического оборудования, построения статистических моделей для нужд мониторинга, обнаружения и локализации отклонений, определения вероятных мест возникновения аварийных ситуаций;

программное обеспечение обработки архивных данных;

программное обеспечение для расширения функциональных возможностей (дополнительные экспертные модули);

программное обеспечение для синхронизации данных.

Для программного обеспечения по сбору данных телеметрии с нижнего уровня СУМиД, накопления и передачи данных на верхний уровень СУМиД, формирования запросов на верхний уровень, анализа технического состояния основного технологического оборудования, который не осуществляется на иных уровнях СУМиД, предварительной обработки предупредительных сообщений, формирования отчетов (программное обеспечение СУМиД среднего уровня) субъект электроэнергетики должен использовать следующие компоненты:

прикладное программное обеспечение сервера хранения данных;

системное программное обеспечение сервера хранения данных;

интерфейсы автоматизированных рабочих мест персонала (интерфейсы автоматизированных рабочих мест для разработки и поддержания в актуальном состояния математических моделей должны применяться для организаций, предоставляющих услугу удаленного мониторинга и диагностики основного технологического оборудования);

программное обеспечение для синхронизации данных между уровнями СУМиД.

Для программного обеспечения СУМиД для временного хранения информации, передачи данных на верхние уровни (программное обеспечение СУМиД нижнего уровня) субъект электроэнергетики должен использовать следующие компоненты:

прикладное программное обеспечение сервера оперативного хранения данных;

системное программное обеспечение сервера оперативного хранения данных.

Если субъектом электроэнергетики в целях выполнения организационных требований к СУМиД используются компоненты СУМиД, не указанные в настоящем пункте, субъект электроэнергетики должен использовать иные компоненты СУМиД.

Если субъектом электроэнергетики в целях выполнения организационных требований к СУМиД не используется полный перечень компонентов СУМиД, указанных в настоящем пункте, то субъект электроэнергетики должен применять используемые компоненты СУМиД с учетом архитектуры СУМиД.

8. Для обеспечения доступа персонала к программному обеспечению СУМиД субъект электроэнергетики должен предусмотреть процедуры идентификации и аутентификации. В процедурах идентификации и аутентификации субъектом электроэнергетики должна быть утверждена политика паролей, соответствующая следующим минимальным требованиям:

минимальная длина пароля должна быть не менее десяти символов, при формировании пароля должны использоваться числовые, буквенные (латиница и (или кириллица, прописные и (или) строчные) и специальные символы;

в целях единовременного входа при формировании временных паролей обновление не должно производиться;

в целях постоянного доступа при формировании пароля доступа обновление должно осуществляться не менее одного раза в квартал.

При обеспечении доступа персонала к программному обеспечению СУМиД субъект электроэнергетики должен предусмотреть следующие минимальные требования:

создать учетные записи, соответствующие требованиям политики паролей, в целях использования программного обеспечения СУМиД для персонала;

утвердить настройки учетных записей персонала;

отключить встроенные учетные записи (неперсонифицированные учетные записи).

9. Для определения и утверждения состава аппаратной инфраструктуры СУМиД и обеспечения процессов контроля за аппаратной инфраструктурой СУМиД субъект электроэнергетики должен предусмотреть процедуры по поддержке организации основных функций СУМиД с учетом необходимости:

обеспечения поддержки технологических процессов конечным набором программного обеспечения, перечень которого утверждается субъектом электроэнергетики;

обеспечения организационных и технических мер регистрации событий безопасности для всего программного обеспечения, входящего в состав СУМиД;

определения и настройки параметров обновления (временной интервал) программного обеспечения для информационной безопасности.

10. Субъектом электроэнергетики должен быть создан архив проектной и эксплуатационной документации для СУМиД. Проектная и эксплуатационная документация должна актуализироваться субъектом электроэнергетики.

11. Состав оборудования аппаратного обеспечения СУМиД, а также программного обеспечения, используемого для аппаратной инфраструктуры, должен утверждаться субъектом электроэнергетики в форме перечня оборудования и программного обеспечения, разрешенного к использованию.

12. Субъект электроэнергетики для выполнения организационных требований к обеспечению информационной безопасности СУМиД основного технологического оборудования должен выполнять процедуру формирования набора сегментов аппаратной инфраструктуры СУМиД (далее – сегментация).

По результатам сегментации аппаратная инфраструктура СУМиД должна включать в себя минимальный набор сегментов, состоящий из:

сегмента сбора, хранения и передачи данных – программного и аппаратного обеспечения нижнего уровня;

сегмента эксплуатации – программного и аппаратного обеспечения среднего уровня;

сегмента обслуживания – программного и аппаратного обеспечения верхнего уровня;

системного программного обеспечения – программного обеспечения, которое обеспечивает управление аппаратными компонентами технических средств и функционирование программного обеспечения.

После выполнения процедуры сегментации субъект электроэнергетики должен определить процессы управления информационной безопасностью СУМиД:

информационно-телекоммуникационной инфраструктурой СУМиД;

комплексом технических средств защиты информации;

программным обеспечением и аппаратными средствами СУМиД.

13. Субъект электроэнергетики должен определить порядок физического доступа персонала объекта электроэнергетики к сегментам аппаратной инфраструктуры СУМиД, который должен быть включен в правила определения и утверждения состава аппаратной инфраструктуры СУМиД и обеспечения контроля за аппаратной инфраструктурой СУМиД.

В целях физического доступа персонала объекта электроэнергетики к сегментам аппаратной инфраструктуры СУМиД необходимо предусмотреть требования по порядку физического доступа персонала в зависимости от функций управления:

информационно-телекоммуникационной инфраструктурой СУМиД;

комплексом технических средств защиты информации;

программным и аппаратным обеспечением СУМиД.

Список разрешенного к использованию программного обеспечения должен утверждаться субъектом электроэнергетики с учетом пунктов 7 и 8 настоящих требований. Использование программного обеспечения, не внесенного в списки разрешенного к использованию, не допускается.

Для серверного оборудования и автоматизированных рабочих мест персонала субъекта электроэнергетики, выполняющего функции управления комплексом технических средств защиты информации, информационно-телекоммуникационной инфраструктуры СУМиД, должны быть обеспечены следующие меры информационной безопасности СУМиД:

включены персональные межсетевые экраны, которые должны обеспечивать блокировку сетевого доступа, не предусмотренного функционированием СУМиД;

установлены пароли для доступа персонала к программному обеспечению и актуальные средства антивирусной защиты с обновлениями.

14. Для предотвращения угроз информационной безопасности СУМиД в отношении аппаратной инфраструктуктуры СУМиД субъектом электроэнергетики должна обеспечиваться безопасность ее функционирования.

Для обеспечения безопасности функционирования аппаратной инфраструктуры СУМиД субъект электроэнергетики должен:

реализовать минимальный комплекс мероприятий для обеспечения безопасности среды функционирования аппаратной инфраструктуры СУМиД организационных требований к обеспечению информационной безопасности аппаратной инфраструктуры СУМиД в соответствии с таблицей 1 приложения № 1 к настоящим требованиям;

применять средства защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности защиты информации, сертифицированные в соответствии с Федеральным законом от 27.12.2002№ 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, № 52, ст. 5140; 2005, № 19, ст. 1752; 2007, № 19, ст. 2293; № 49, ст. 6070; 2008, № 30, ст. 3616; 2009, № 29, ст. 3626; № 48, ст. 5711; 2010, № 1, ст. 5, 6; № 40, ст. 4969; 2011, № 30, ст. 4603; № 49, ст. 7025; № 50, ст. 7351; 2012, № 31, ст. 4322; № 50, ст. 6959; 2013, № 27, ст. 3477; № 30, ст. 4071; № 52, ст. 6961; 2014, № 26, ст. 3366; 2015, № 17, ст. 2477; № 27, ст. 3951; № 29, ст. 4342; № 48, ст. 6724; 2016, № 15, ст. 2066, 2017, № 27, ст. 3938, № 31, ст. 4765) (далее – Федеральный закон № 184-ФЗ).

15. Для определения и утверждения состава аппаратной инфраструктуры СУМиД и обеспечения процессов контроля за аппаратной инфраструктурой СУМиД субъект электроэнергетики должен руководствоваться требовании пунктов 9-14 настоящих требований.

16. Для обеспечения информационной безопасности встроенных средств защиты информации в отношении СУМиД в качестве меры по обеспечению предотвращения угроз информационной безопасности СУМиД субъектом электроэнергетики должна проводиться проверка соответствия встроенных средств защиты информационной безопасности СУМиД следующим целям информационной безопасности СУМиД:

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.

Описание целей информационной безопасности СУМиД организационных требований к обеспечению контроля информационной безопасности СУМиД приведено в таблице 2 приложения № 1 к настоящим требованиям.

17. Для обеспечения контроля информационной безопасности СУМиД субъектом электроэнергетики должен быть предусмотрен контроль соответствия и исполнения требований информационной безопасности СУМиД.

В целях обеспечения мер по предотвращению утечек информации, сбор, обработка и хранение которой осуществляется СУМиД, субъект электроэнергетики должен реализовываться комплекс мероприятий по:

контролю проектной документации и исходного состояния программного обеспечения;

защите от несанкционированного доступа к информации о технических и технологических параметрах основного технологического оборудования;

обеспечению формирования и хранения отчетности указанных мероприятий.

18. В качестве базового набора средств контроля информационной безопасности СУМиД субъект электроэнергетики должен:

утвердить политику информационной безопасности для СУМиД, сформированную в соответствии с главой III настоящих требований;

распределить обязанности по обеспечению информационной безопасности СУМиД внутри организации;

проводить обучение и подготовку персонала по обеспечению информационной безопасности СУМиД;

проводить обучение и подготовку персонала по поддержанию режима информационной безопасности СУМиД;

организовать процессы уведомления о случаях нарушения защиты СУМиД;

применять для СУМиД средства защиты от исполняемых (компьютерных, программных) кодов или интерпретируемых наборов инструкций, обладающих свойством несанкционированного распространения и самовоспроизведения (вирусы);

обеспечивать защиту данных и проектной документации СУМиД;

осуществлять контроль соответствия СУМиД утвержденной политике информационной безопасности.

19. Для обеспечения контроля информационной безопасности СУМиД субъект электроэнергетики должен руководствоваться требованиями пунктов 17 и 18 настоящих требований.

20. Субъектом электроэнергетики должно проводиться категорирование СУМиД в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) и 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 и их значений» (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

21. Субъектом электроэнергетики в отношении СУМиД должны выполняться требования к организационно-распорядительным документам по безопасности значимых объектов критической информационной инфраструктуры Российской Федерации в соответствии с главой IV Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 (зарегистрирован Минюстом России 22.02.2018, регистрационный № 50118) (далее – Требования к созданию систем безопасности).

III. Требования к обеспечению информационной безопасности систем удаленного мониторинга и диагностики при их создании и последующей эксплуатации

22. 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», утвержденным и введенным в действие постановлением Госстандарта СССР от 29.12.1990 № 3469 (ИПК Издательство стандартов, 1997).

23. Для обеспечения информационной безопасности СУМиД при создании и последующей эксплуатации СУМиД функция технологического мониторинга состояния основного технологического оборудования в части сбора, хранения и передачи данных должна осуществляться посредством инфраструктуры сбора, хранения и передачи данных (центров обработки данных), расположенной на территории Российской Федерации.

Если при реализации функции технологического мониторинга состояния основного технологического оборудования при передаче данных эксплуатируются сети связи общего пользования, то при передаче данных должны использоваться средства защиты информации, прошедшие оценку соответствия в соответствии с требованиями Федерального закона № 184-ФЗ.

24. Если в СУМиД предусмотрена функция удаленного управления основным технологическим оборудованием с использованием специального программного обеспечения и/или модуля программного обеспечения СУМиД, 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.

25. Требования к обеспечению информационной безопасности СУМиД должны соблюдаться субъектом электроэнергетики вместе с требованиями к моделированию угроз и функциональными требованиями, предусмотренными пунктами 26 – 29 настоящих требований.

26. Для моделирования угроз информационной безопасности СУМиД субъекту электроэнергетики необходимо выполнить процедуру моделирования и описать базовую модель угроз информационной безопасности СУМиД.

Для моделирования угроз информационной безопасности СУМиД субъект электроэнергетики должен оценивать существующие уязвимости СУМиД и её компонентов, вероятность угроз и их реализацию (использование), опасности

рассматриваемой угрозы с точки зрения потенциальных последствий и деструктивных действий, выполняемых в результате реализации угроз.

Для моделирования угроз информационной безопасности СУМиД субъект электроэнергетики должен использовать:

банк данных угроз безопасности информации, 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; 2018, № 20, ст. 2818), 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 моделирования угроз информационной безопасности субъект электроэнергетики должен сформировать перечень актуальных угроз информационной безопасности СУМиД.

27. По результатам моделирования угроз информационной безопасности СУМиД субъектом электроэнергетики должна быть разработана модель угроз информационной безопасности СУМиД, на основании которой формируется политика информационной безопасности. Политика информационной безопасности СУМиД должна включать в себя функциональные требования к информационной безопасности СУМиД.

Для разработки модели угроз информационной безопасности СУМиД субъект электроэнергетики должен использовать:

описание СУМиД, характеристики функций СУМиД, результаты процедуры сегментации;

описание источников угроз, типовых уязвимостей, объектов воздействия, деструктивных действий в отношении СУМиД;

модели нарушителя информационной безопасности СУМиД.

При описании источников угроз информационной безопасности СУМиД субъектом электроэнергетики должны использоваться следующие источники угроз информационной безопасности СУМиД:

конкуренты;

криминальные элементы (структуры);

недобросовестные партнеры;

работники (персонал) организации (субъекта электроэнергетики);

лица, осуществляющие создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

разработчики и производители технических средств и программного обеспечения.

Для определения типовых угроз СУМиД субъектом электроэнергетики должен быть проведен анализ уязвимостей в отношении:

семейства протоколов, предоставляющих интерфейс для управления объектами автоматизации и технологическими процессами;

прикладного программного обеспечения, систем управления базами данных;

операционных систем.

Для проведения анализа уязвимостей необходимо использовать перечни:

базовых атак, необходимых при анализе уязвимостей и построении модели угроз СУМиД, приведенных в таблице 1 приложения № 2 к настоящим требованиям;

базовых уязвимостей СУМиД, необходимых для проведения анализа уязвимостей СУМиД и построения модели угроз СУМиД, приведенных в таблице 2 приложения № 2 к настоящим требованиям.

Для описания основных объектов воздействия СУМиД необходимо применять следующий перечень объектов воздействия:

а) серверы автоматизированой системы управления и СУМиД среднего и нижнего уровней;

б) сетевой контур взаимодействия между:

сервером СУМиД нижнего уровня и автоматизированным рабочим местом персонала;

серверами СУМиД нижнего, среднего и верхнего уровней;

сервером СУМиД верхнего уровня и прикладным программным обеспечением (средства обработки данных и разработки математических моделей);

сервером СУМиД и автоматизированным рабочим местом персонала.

Субъект электроэнергетики вправе определять дополнительные объекты воздействия СУМиД.

Определение возможных деструктивных действий в отношении безопасности информации СУМиД для каждой из угроз информационной безопасности СУМиД должны осуществляться субъектом электроэнергетики в соответствии с приложением № 3 к настоящим требованиям.

Для определения основных деструктивных действий в отношении информационной безопасности СУМиД субъект электроэнергетики должен использовать следующие деструктивные действия:

несанкционированное копирование информации (деструктивное действие 1 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

уничтожение информации (носителя информации) (деструктивное действие 2 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

модифицирование информации (изменение исходной информации на ложную) (деструктивное действие 3 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

блокирование информации (деструктивное действие 4 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

перехват информации при ее передаче по каналам связи (деструктивное действие 5 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

разглашение информации персоналом (деструктивное действие 6 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

хищение носителя информации (деструктивное действие 7 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

нанесение ущерба здоровью персонала и окружающим людям (деструктивное действие 8 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

нанесение ущерба окружающей среде (деструктивное действие 9 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

физическое повреждение объекта защиты или его компонент (деструктивное действие 10 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям);

блокирование контроля над объектом защиты (деструктивное действие 11 в соответствии с нумерацией, приведенной в приложении № 3 к настоящим требованиям).

Субъект электроэнергетики вправе определять дополнительные деструктивные действия в отношении СУМиД.

28. Для обеспечения контроля информационной безопасности компонент СУМиД, приведенных в пункте 7 настоящих требований, и персонала субъект электроэнергетики должен установить модель нарушителя информационной безопасности СУМиД.

Модели нарушителей информационной безопасности СУМиД должны быть утверждены субъектом электроэнергетики.

Виды нарушителей для определения модели нарушителей информационной безопасности СУМиД приведены в приложении № 4 к настоящим требованиям.

29. Для достижения целей информационной безопасности СУМиД субъектом электроэнергетики должны устанавливаться функциональные требования к информационной безопасности СУМиД.

30. Для подтверждения соответствия СУМиД настоящим требованиям субъектом электроэнергетики должна проводиться оценка СУМиД и её подсистемы безопасности в форме аттестации СУМиД 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 (зарегистрирован Минюстом России 31.05.2013, регистрационный № 28608), с изменениями, внесеннными приказом ФСТЭК России от 15.02.2017 № 27 (зарегистрирован Минюстом России 14.03.2017, регистрационный № 45933) (далее – Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах).

31. 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 (зарегистрирован Минюстом России 26.03.2018, регистрационный № 50524), с изменениями, внесенными приказом ФСТЭК России от 09.08.2018 № 138 (зарегистрирован Минюстом России 05.09.2018, регистрационный № 52071), а также Требованиями к созданию систем безопасности с учетом пунктов 23-24 настоящих требований.

32. Для обеспечения системы информационной безопасности СУМиД субъектом электроэнергетики должны устанавливаться требования ко встроенным стредствам защиты.

Для обеспечения системы безопасности компонент СУМиД субъект электроэнергетики должен выполнять требования, установленные главой III Требований к созданию систем безопасности.

При организации работ по обеспечению безопасности СУМиД в рамках функционирования системы безопасности субъект электроэнергетики должен выполнять требования, установленные главой V Требований к созданию систем безопасности.

33. Ввод в действие СУМиД и ее подсистемы безопасности должен осуществляться после получения аттестата соответствия СУМиД.*

*Пункт 17.5. Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Приложение № 1
к требованиям 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

Мероприятия по обеспечению безопасности среды функционирования аппаратной инфраструктуры СУМиД и цели информационной безопасности

Таблица 1. Минимальный комплекс мероприятий для обеспечения безопасности среды функционирования аппаратной инфраструктуры СУМиД организационных требований к обеспечению информационной безопасности аппаратной инфраструктуры СУМиД

№ п/п	Мероприятие	Описание
1.	Контроль физического доступа	В местах размещения аппаратной инфраструктуры СУМиД должен быть обеспечен контроль физического доступа.
2.	Безопасная установка	Процесс установки, инсталляции и администрирования аппаратной инфраструктуры, программного обеспечения СУМиД должен соответствовать требованиям политики информационной безопасности, утвержденной собственником или иным законным владельцем объекта электроэнергетики. Контроль соответствия требований информационной безопасности осуществляется субъектом электроэнергетики.
3.	Повышение осведомленности	Администраторы СУМиД должны пройти обучение способам администрирования программного обеспечения и получить сертификат об окончании обучения. В составе программы обучения должны входить мероприятия по получению знаний и навыков реализации требований информационной безопасности, действующих в Российской Федерации.

4.	Администрирование безопасности	В рамках организационной структуры подразделения, эксплуатирующего программное обеспечение, должна быть предусмотрена роль администратора информационной безопасности. Роль администратора информационной безопасности должна быть регламентирована и утверждена субъектом электроэнергетики. В качестве исполнителя роли администратора информационной безопасности может быть только сотрудник объекта в соответствии со штатным расписанием.

Таблица 2. Описание целей информационной безопасности СУМиД, организационных требований к обеспечению контроля информационной безопасности СУМиД

№ п/п	Цель информационной безопасности	Идентификатор	Описание
1.	Аудит событий	O.AUDITING	Программное обеспечение должно обеспечивать: а) генерацию, запись и хранение событий информационной безопасности относящихся к функционированию встроенных средств защиты (при этом генерация, запись и хранение событий информационной безопасности должны осуществляться за счет инфраструктуры, расположенной на территории Российской Федерации); б) защиту данных журналов (доступ к журналам разрешен пользователям, имеющим право допуска, правила получения, которого устанавливаются субъектом электроэнергетики). Информация, хранящаяся в журналах, должна содержать: а) дату (день, месяц и год) и время (часы, минуты, секунды) произошедшего события информационной безопасности, идентификационные данные пользователя, от имени которого совершалось действие или был запущен процесс, повлекший наступление события информационной безопасности; б) подробное описание предпринимаемых действий для последующего их анализа, выявления попыток несанкционированного доступа или несанкционированной модификации компонент программного обеспечения.

2.	Криптографическая защита	O.CRYPTO	Программное обеспечение должно обеспечивать целостность и конфиденциальность информации. Целостность и конфиденциальность информации обеспечиваются средствами криптографической защиты. Удаленное соединение должно обеспечиваться совместно со средствами криптографической защиты. В рамках открытых сессий обмена данными должны использоваться средства криптографической защиты. В случае с распределенной сетью хранения и получения данных должны использоваться средства криптографической защиты.
3.	Дискретный доступ	O.DACCESS	Программное обеспечение должно осуществлять контроль доступа персонала на основе идентификаторов объектов. Доступ к объектам пользователей должен осуществляться на основании правил доступа персонала к объектам.
4.	Контроль сетевого взаимодействия	O.NFLOW	Программное обеспечение должно осуществлять контроль взаимодействия и передачи информации между сетевыми интерфейсами (в том числе виртуальными), между субъектами, между внутренними функциями на основании настраиваемой политики безопасности в рамках функций СУМиД.
5.	Передача атрибутов безопасности	O.SUBJECT	При взаимодействии пользователей программное обеспечение должно обеспечивать передачу атрибутов безопасности в соответствии с настраиваемой политикой безопасности.
6.	Идентификация и аутентификация	O.I&A	Программное обеспечение должно обеспечивать идентификацию и аутентификацию пользователей для любых действий на основе сертификата открытого ключа подписи и связанного с ним закрытого ключа подписи, размещенного на отчуждаемом носителе. Доступ к программному обеспечению СУМиД должен предоставляться только авторизованным пользователям. Должна быть обеспечена многофакторная аутентификация с использованием доступных для субъектов электроэнергетики средств.

7.	Конфигурация безопасности	O.MANAGE	Программное обеспечение должно содержать необходимые механизмы для управления и настройки всех имеющихся функций безопасности. Доступ к этим механизмам должен быть обеспечен только авторизованным пользователям с выделенной ролью администратора информационной безопасности. Программное обеспечение должно иметь возможность указывать на ошибки персонала при конфигурации, а также должно запрещать возможность снижения уровня безопасности. Применяемые средства защиты информации должны соответствовать пунктам 19-22 Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 (зарегистрирован Минюстом России 22.02.2018, регистрационный № 50118).
8.	Установление защищенных соединений	O.TRUSTCHAN	Программное обеспечение должно быть спроектировано и разработано таким образом, чтобы позволять установление защищенного соединения с информационными системами того же класса доверия, гарантируя при этом целостность, доступность и конфиденциальность передаваемых в рамках соединения данных, взаимную авторизацию и возможность обмена атрибутами безопасности.
9.	Доступность	O.AVAIL	Функционирование программного обеспечения должно осуществляться на постоянной основе. В случае выходов из строя каналов связи функционирование программного обеспечение должно продолжаться. Должны быть предусмотрены механизмы обеспечения продолжения функционирования при переполнении баз данных. Должен осуществляться контроль целостности компонентов СУМиД в процессе их загрузки и эксплуатации. Должно быть исключено неконтролируемое, несанкционированное вмешательство в процессы перезагрузки

			или восстановления после сбоев компонентов программного обеспечения СУМиД. В процессе функционирования программного обеспечения СУМиД должны быть предусмотрены на периодической основе проверки на наличие уязвимостей компонентов программного обеспечения СУМиД. Должны быть предусмотрены возможности восстановления данных и (или) параметров конфигураций компонентов программного обеспечения СУМиД из резервных копий в случае их компрометации, уничтожения, ошибочного изменения, замены аппаратного обеспечения СУМиД. Должны быть предусмотрены возможности создания резервных копий в случае внесения изменений в конфигурации, с заданной периодичностью или комбинации этих вариантов персоналом субъекта электроэнергетики вручную или автоматически с использованием прикладного программного обеспечения.

Приложение № 2
к требованиям 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

Базовые атаки и базовые уязвимости для построения модели угроз СУМиД

Таблица 1. Перечень базовых атак, необходимых при анализе уязвимостей и построении модели угроз СУМиД

№ п/п	Объект атаки	Тип атаки	Результат атаки
1.	Атаки вследствие использования стека протокола IPSec, PPTP, L2TP, SSL	Атаки типа «человек в середине» и «отказ в обслуживании»	Возможность получения прав администратора, нарушение конфиденциальности, целостности, доступности защищаемой информации
2.	Атаки вследствие использования стека протоколов TCP, UDP	Атаки типа «отказ в обслуживании» и «инъекция данных»	Возможность сканирования портов
3.	Атаки вследствие использования стека протоколов OPC, TELNET, SSH, VNC, RADMIN, TEAMVIEWER, LYNC терминальный доступ (RS-232), HP iLO	Атаки типа «отказ в обслуживании», атаки через неизвестные или неклассифицированные векторы	Неизвестен
4.	Атаки вследствие использования стека протоколов FTP, SMB, CIFS, TACA, SFTP, Rsync	Атаки, направленные на получение прав администратора, связанные с выполнением произвольного кода типа «отказ в обслуживании»	Возможность получения прав администратора
5.	Атаки вследствие использования серверами СУМиД программного обеспечения MS Windows, терминального доступа	Атаки, связанные с: выполнением злоумышленникам произвольного кода, повышением злоумышленниками своих привилегий, возможностью обхода	Неизвестен

		процедуры аутентификации, позволяющие нарушителю получить доступ к защищаемой информации, обойти механизмы доверенной загрузки, типа «отказ в обслуживании»	

Таблица 2. Перечень базовых уязвимостей СУМиД, необходимых для проведения анализа уязвимостей СУМиД и построения модели угроз СУМиД

№ п/п	Уязвимость
1.	Среда и инфраструктура:
1.1.	отсутствие физической защиты зданий, дверей и окон;
1.2.	неправильное или халатное использование физических средств управления доступом в зданиях и помещениях, а также энергоустановками;
1.3.	нестабильная работа электросети собственных нужд;
1.4.	отсутствие системы обеспечения аварийного электропитания оборудования;
1.5.	отсутствие средств пожарной сигнализации;
1.6.	отсутствие средств пожаротушения;
1.7.	размещение в зонах возможного затопления компонентов систем или энергоустановок.
2.	Линии связи и сетевые подключения:
2.1.	незащищенные линии связи;
2.2.	неудовлетворительная стыковка кабелей, спайка оптоволоконных линий;
2.3.	отсутствие идентификации и (или) аутентификации отправителя и получателя в прикладном программном обеспечении;
2.4.	подмена данных.
3.	Отказ в обслуживании:
3.1.	несанкционированный доступ к каналам связи;
3.2.	перехват информации;
3.3.	получение несанкционированного доступа к учётной информации (в том числе к учетным данным пользователей, конфигурационным файлам);
3.4.	получение несанкционированного доступа;
	коммутируемые линии связи и (или) использование сотовых сетей передачи информации, использование технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11;
3.5.	незащищенные потоки конфиденциальной информации;
3.6.	незащищенные подключения к сетям общего пользования.
4.	Сетевое оборудование:
4.1.	отсутствие средств для маршрутизации в целях безопасного управления сетью;
4.2.	ошибки конфигурации сетевых устройств;
4.3.	отсутствие обновлений и патчей на сетевом оборудовании как от производителя, так и не соответствие установленных версий с официальными версиями производителя;
4.4.	неправильная сетевая топология (например, использование «плоских» локальных сетей);
4.5.	использование паролей с малым набором символов, «паролей по умолчанию» или ненадежных механизмов аутентификации на сетевом оборудовании;

4.6.	отказ системы вследствие отказа одного из ключевых элементов телекоммуникационного оборудования или агрегирующего контроллера (угроза сбоев в функционировании услуг связи).
5.	Аппаратное обеспечение:
5.1.	отсутствие схем периодической замены оборудования СУМиД по истечении срока его полезного использования;
5.2.	подверженность колебаниям напряжения оборудования СУМиД;
5.3.	подверженность температурным колебаниям оборудования СУМиД;
5.4.	подверженность воздействию влаги, пыли, загрязнения оборудования СУМиД;
5.5.	чувствительность к воздействию электромагнитного излучения оборудования СУМиД;
5.6.	недостаточное обслуживание / неправильная инсталляция запоминающих сред (в том числе систем хранения данных) СУМиД;
5.7.	отсутствие контроля за эффективным изменением конфигурации оборудования или телекоммуникационного оборудования сетей связи в СУМиД;
5.8.	отсутствие контроллера версии прошивок firmware (версионирование).
6.	Программное обеспечение:
6.1.	отсутствие технических требований к разработке программного (программно-аппаратного) обеспечения, применяемого в СУМиД;
6.2.	отсутствие тестирования или упрощенное тестирование программного обеспечения (угроза использования программного обеспечения несанкционированными пользователями);
6.3.	сложный пользовательский интерфейс компонентов мониторинга и управления энергосетью (угроза ошибки операторов);
6.4.	отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей;
6.5.	отсутствие внешней аудиторской проверки установленного программного обеспечения;
6.6.	ошибки конфигурации программного обеспечения;
6.7.	неустановленные патчи и обновления программного обеспечения (в том числе системного программного обеспечения);
6.8.	отсутствие системы управление паролями учетных записей операторов, управление паролями оборудования, в том числе программируемых контроллеров (определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей);
6.9.	неправильное присвоение прав доступа (угроза использования программного обеспечения несанкционированным способом);
6.10.	неконтролируемая загрузка, установка и использование программного обеспечения (угроза столкновения с вредоносным программным обеспечением);
6.11.	отсутствие регистрации окончания сеанса при выходе с рабочей станции (угроза использования программного обеспечения несанкционированными пользователями);
6.12.	отсутствие эффективного контроля внесения изменений (угроза программных сбоев);
6.13.	отсутствие документации (угроза ошибки операторов в связи с отсутствием алгоритмов действий);
6.14.	отсутствие резервных копий информации, обрабатываемой в системе;
6.15.	списание или повторное использование запоминающих сред без надлежащего стирания записей;
6.16.	наличие недекларированных возможностей (программных и аппаратных закладок)

	в оборудовании иностранных производителей.
7.	Документация:
7.1.	хранение в незащищенных местах (угроза хищения документации);
7.2.	недостаточная внимательность при уничтожении (угроза хищения документации);
7.3.	бесконтрольное копирование (угроза хищения документации).
8.	Персонал:
8.1.	отсутствие квалифицированного персонала (угроза халатного отношения работников к своим обязанностям);
8.2.	отсутствие надзора за работой лиц, приглашенных со стороны, или за работой обслуживающего персонала (угроза хищения документации, данных, информации);
8.3.	отсутствие механизмов отслеживания и мониторинга для обеспечения устойчивости программного обеспечения к несанкционированному использованию (угроза использования программного обеспечения несанкционированным способом);
8.4.	отсутствие политики и (или) наличие ошибок в политике допустимого использования телекоммуникационных систем для обмена сообщениями (угроза использования сетевых средств несанкционированным способом);
8.5.	несоответствующие процедуры набора кадров (угроза намеренного повреждения или недостаточной квалификации дежурного и оперативного персонала).

Приложение № 3
к требованиям 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

Возможные деструктивные действия в отношении безопасности информации СУМиД для каждой из угроз информационной безопасности СУМиД

№ п/п	Код угрозы информационной безопасности	Угроза информационной безопасности	Деструктивное действие										
			1	2	3	4	5	6	7	8	9	10	11
1.	УФД1	Физическое проникновение на территорию без возможности проникновения в помещения с техническими средствами обработки, носителями информации, энергоустановок		+								+	+
2.	УФД2	Хищение носителя информации, средств обработки информации (процессора, микросхемы, контроллеров, серверов), средств коммуникации (маршрутизатора, коммутатора, сетевой карты, модема), средств ввода вывода информации (клавиатура)	+	+	+	+			+				+
3.	УФД3	Уничтожение носителя информации, средств обработки информации		+									+

		(процессора, микросхемы, контроллеров, серверов), средств коммуникации (маршрутизатора, коммутатора, сетевой карты, модема), средств ввода вывода информации (клавиатура)											
4.	УФД4	Потеря носителя информации	+	+		+							+
5.	УФД5	Чтение информации с устройств отображения						+					
6.	УФД6	Повреждение оборудования и (или) линий связи				+						+	+
7.	УФД7	Навязывание ложной информации на уровне конечного оборудования или линий связи (при обмене данными между датчиками и контроллерами, между контроллерами и автоматизированной системой управления)			+	+							+
8.	УФД8	Съем информации с конечного оборудования или линий связи (датчиков, контроллеров)	+				+						
9.	УФД9	Захват объекта защиты, установление над объектом защиты контроля силой или угрозой применения силы, или путем любой другой формы запугивания								+			+
10.	УФД10	Разрушение								+		+	+

		объекта защиты или нанесение объекту защиты, здоровью персонала и другим лицам повреждений путем взрыва (обстрела)											
11.	УФД11	Размещение и (или) совершение действий в целях размещения на объекте защиты взрывных устройств (взрывчатых веществ)								+		+	+
12.	УФД12	Загрязнение объекта защиты опасными веществами, угрожающими жизни и здоровью персонала и других лиц								+	+		
13.	УНДА1	Подбор пароля BIOS или системного программного обеспечения контроллера путем перебора вручную на основе предварительно собранных данных о пользователе	+		+								
14.	УНДА2	Обход заданного пароля BIOS или системного программного обеспечения контроллера (воздействие на аппаратное обеспечение)	+		+								
15.	УНДА3	Загрузка альтернативной операционной системы с нештатного носителя	+		+	+							
16.	УНДБ1	Подбор пароля	+		+	+							

		доступа (администратора) в операционную систему компьютера или к системному программному обеспечению контроллера с использованием заданных по умолчанию значений («заводских» паролей)											
17.	УНДБ1.2	Подбор пароля доступа (администратора) в операционную систему компьютера или к системному программному обеспечению контроллера посредством перебора различных вариантов	+		+								
18.	УНДВ	Подбор пароля доступа (администратора) в операционную систему компьютера посредством специализированно-го программного обеспечения	+		+								+
19.	УНДГ1	Выявление пароля BIOS при загруженной операционной системе, посредством использования программ выявления пароля	+		+								
20.	УНДГ2	Выявление пароля доступа других пользователей при загруженной	+		+								

		операционной системе (декодирование, из оперативной памяти, копирование хранилищ)											
21.	УНДГ3	Создание новой учетной записи с расширенными привилегиями	+		+								+
22.	УНДГ4	Уничтожение системного реестра, обнуление памяти контроллера				+							+
23.	УНДГ5	Редактирование системного реестра с целью нарушения работоспособности операционной системы и (или) прикладного программного обеспечения	+		+	+							+
24.	УНДГ6	Использование стороннего программного обеспечения с целью несанкционированного воздействия на объект защиты	+		+	+							+
25.	УНДГ6.4	Заражение вредоносным программным обеспечением автоматизированных рабочих мест, серверов, контроллеров	+	+	+	+							+
26.	УНДГ7	Перезагрузка операционной системы с целью загрузки альтернативной операционной системы с нештатного носителя для расширения привилегий	+		+	+							+

27.	УНДГ8	Копирование информации на нештатные носители информации	+										
28.	УНДГ9	Модификация информации			+								
29.	УНДГ10	Уничтожение (стирание) информации		+		+							+
30.	УНДГ11	Уничтожение информации путем форматирования носителей информации		+									+
31.	УУДА1	Сканирование сегмента сети с целью сбора информации	+										
32.	УУДБ1	Удаленный подбор пароля (администратора) посредством ввода имени и пароля, заданных по умолчанию для используемой операционной системы	+		+								
33.	УУДБ1.2	Удаленный подбор имени и пароля (администратора) посредством перебора	+		+	+							+
34.	УУДБ2	Удаленный подбор пароля (пользователя)	+										
35.	УУДБ3	Получение доступа к программам удаленного администриро-вания	+		+	+							+
36.	УУДБ4	Внедрение ложного доверенного объекта	+		+	+							+
37.	УУДБ5	Угрозы удаленного перехвата внешнесегментного сетевого трафика	+				+						
38.	УУДБ5.3	Удаленный перехват аутентификацион-	+										

		ной информации, передаваемой в открытом виде											
39.	УУДВ2	Переполнение буфера с запуском исполняемого кода	+		+	+							
40.	УУДВ10	Перенаправление сетевого трафика	+		+		+						
41.	УУДГ	Атаки на узлы, подключенные к сети информационно-телекоммуникационной сети «Интернет»	+	+	+	+							+
42.	УУДД	Угрозы отказа в обслуживании (DoS)				+							+
43.	УУДЕ1	Обход межсетевого экрана посредством инкапсуляции данных в заголовки пакетов протокола обмена сообщениями	+		+	+							+
44.	УМУ1	Хищение мобильного устройства	+										
45.	УМУ2	Потеря мобильного устройства	+										
46.	УМУ3	Несанкционированное считывание информации с дисплея мобильного устройства	+										
47.	УМУ4	Внедрение вредоносного программного обеспечения на мобильное устройство	+		+								
48.	УМУ5	Перехват паролей при доступе с мобильного устройства через незащищенные сети, а также использование мобильного устройства в незащищенных	+			+							

		сетях											
49.	УМУ6	Выявление хранящихся на мобильном устройстве паролей	+			+							
50.	УО1	Ошибки при проектировании программного обеспечения	+	+	+	+							+
51.	УО2	Ошибки при проектировании технических средств	+	+	+	+							+
52.	УО3	Ошибки при изготовлении программного обеспечения	+	+	+	+							
53.	УО4	Ошибки при изготовлении технических средств	+	+	+	+							
54.	УО5	Ошибки при эксплуатации технических средств	+	+	+	+							+
55.	УО6	Ошибки при эксплуатации программного обеспечения	+	+	+	+							+
56.	УТХ1	Сбои, отказы технических средств				+							+
57.	УТХ2	Сбои, отказы программного обеспечения				+							+
58.	УБИЛ80	Отказ подсистемы обеспечения температурного режима		+								+	+
59.	УБИЛ82	Физическое устаревание компонентов аппаратного обеспечения											+

Приложение № 4
к требованиям 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

ВИДЫ НАРУШИТЕЛЕЙ
для определения модели нарушителей информационной безопасности СУМиД

№ п/п	Основные направления для установления модели нарушителя	Вид нарушителя	Описание нарушителя
1.	По отношению к СУМиД	Внутренний	Лицо с разрешенным доступом к компонентам системы СУМиД и с разрешенным доступом на территорию объекта электроэнергетики (эксплуатация, постановка, сопровождение, обслуживание и ремонт аппаратного обеспечения).
		Внешний	Постороннее лицо, разрабатывающее/распространяющее вирусы и другие программы, предназначенные для осуществления несанкционированного доступа и (или) воздействия на ресурсы и информацию, хранимую на ресурсах, с целью несанкционированного использования или причинения вреда (нанесения ущерба) владельцу информации, ресурса путем копирования, искажения, удаления или подмены информации программы; лицо, организующее атаки на отказ в обслуживании.
		Иной нарушитель	Лицо, осуществляющее попытки несанкционированного доступа к СУМиД.

2.	По правам доступа к компонентам СУМиД	Авторизованный (зарегистрированный) пользователь, системный администратор, администратор безопасности компонент СУМиД	Лицо, имеющее разрешенный доступ к компонентам СУМиД.
		Иной нарушитель	Лицо, не имеющее прав доступа к компонентам СУМиД.
3.	По мотивации нарушения	С немотивированными действиями	Действия или бездействие пользователей без злого умысла, связанные со случайным нарушением свойств информационной безопасности информационных активов.
		Действия в целях самоутверждения	Действия пользователя, приводящие к нарушению свойств безопасности СУМиД, в целях самоутверждения.
		Корыстный интерес и терроризм	Действия пользователя, приводящие к нарушению свойств безопасности информационных активов, направленные на получение выгоды.
4.	По возможностям физического доступа	Без доступа в контролируемую зону	Без доступа в помещения, в которых расположены компоненты СУМиД.
		С доступом в контролируемую зону	С доступом к техническим средствам СУМиД (в том числе за пределами контролируемой зоны); с доступом к рабочему месту администратора СУМиД.
5.	По квалификации	Без знаний	Лицо без знаний об устройстве и особенностях функционирования СУМиД.
		Со знанием	Лицо со знанием функциональных особенностей СУМиД, протоколов передачи информации, основных закономерностей формирования в ней массивов данных и потоков запросов к ним, с умением пользоваться штатными средствами операционных систем, систем управления базами данных и прикладным программным обеспечением.
		С высоким уровнем знаний	Лицо со знанием в области программирования и уязвимостей применяемых технологий обеспечения функционирования СУМиД.

		С обладанием возможностями активного воздействия на СУМиД	Разработчики, профильные эксперты и другие лица.
6.	По направлению реализации угроз информационной безопасности	Реализация угроз направлена на физический вектор	Не требуется.
		Реализация угроз направлена на СУМиД из сети информационно-телекоммуникационной сети «Интернет», корпоративной информационной вычислительной системы	Не требуется.
		Реализация угроз осуществляется с использованием вредоносного программного обеспечения и сетевых атак внутри СУМиД	Не требуется.