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.