ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«9» августа 2018 г.

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Москва
ЗАРЕГИСТРИРОВАНО
Регистрационный № 52071
от "05" сентября 2018 г.

№ 138

О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

Внести в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г.

№ 31 (зарегистрирован Министерством юстиции Российской Федерации 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесёнными приказом Федеральной службы по техническому и экспортному контролю от 23 марта 2017 г. № 49 (зарегистрирован Министерством юстиции Российской Федерации 25 апреля 2017 г., регистрационный № 46487), и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) изменения согласно приложению к настоящему приказу.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Приложение
к приказу ФСТЭК России
от « 9 » августа 2018 г. № 138

Изменения, которые вносятся в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

1. В Требованиях к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31:

1) пункт 1 после абзаца первого дополнить абзацем следующего содержания:

«Обеспечение безопасности автоматизированных систем управления, являющихся значимыми объектами критической информационной инфраструктуры Российской Федерации, осуществляется в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239, а также Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению

их функционирования, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный № 50118).»;

2) абзацы первый – четвертый подпункта 13.3 пункта 13 изложить в следующей редакции:

«13.3. Определение угроз безопасности информации осуществляется на каждом из уровней автоматизированной системы управления и должно включать:

а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

б) анализ возможных уязвимостей автоматизированной системы и входящих в ее состав программных и программно-аппаратных средств;

в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

г) оценку возможных последствий от реализации (возникновения) угроз безопасности информации, нарушения отдельных свойств безопасности информации (целостности, доступности, конфиденциальности) и автоматизированной системы управления в целом.

В качестве исходных данных при определении угроз безопасности информации используется 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 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.»;

3) в подпункте 15.3 пункта 15:

после абзаца второго дополнить абзацем следующего содержания:

«определение администратора безопасности информации;»;

в абзаце четвертом после слов «персонала автоматизированной системы управления» дополнить словами «и администратора безопасности информации»;

4) пункт 18 изложить в следующей редакции:

«18. Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования должны обеспечивать:

идентификацию и аутентификацию (ИАФ);

управление доступом (УПД);

ограничение программной среды (ОПС);

защиту машинных носителей информации (ЗНИ);

аудит безопасности (АУД);

антивирусную защиту (АВЗ);

предотвращение вторжений (компьютерных атак) (СОВ);

обеспечение целостности (ОЦЛ);

обеспечение доступности (ОДТ);

защиту технических средств и систем (ЗТС);

защиту информационной (автоматизированной) системы и ее компонентов (ЗИС);

реагирование на компьютерные инциденты (ИНЦ);

управление конфигурацией (УКФ);

управление обновлениями программного обеспечения (ОПО);

планирование мероприятий по обеспечению безопасности (ПЛН);

обеспечение действий в нештатных ситуациях (ДНС);

информирование и обучение персонала (ИПО).

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности автоматизированных систем управления приведены в приложении № 2 к настоящим Требованиям.

Содержание мер и правила их реализации устанавливаются методическим документом, разработанным ФСТЭК России в соответствии с пунктом 5 и подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.»;

5) подпункты 18.1 – 18.21 пункта 18 признать утратившими силу.

6) приложение № 2 к указанным Требованиям изложить в следующей редакции:

«Приложение № 2
к Требованиям к обеспечению защиты
информации в автоматизированных
системах управления производственными
и технологическими процессами
на критически важных объектах,
потенциально опасных объектах,
а также объектах, представляющих
повышенную опасность для
жизни и здоровья людей
и для окружающей природной среды

**Состав мер защиты информации
и их базовые наборы для соответствующего класса защищенности
автоматизированной системы управления**

Условное обозначение и номер меры	Меры защиты информации в автоматизированных системах управления	Классы защищенности автоматизированной системы управления		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
II. Управление доступом (УПД)				
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступа	+	+	+

УПД.3	Доверенная загрузка		+	+
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам			
УПД.8	Оповещение пользователя при успешном входе предыдущем доступе к информационной (автоматизированной) системе			+
УПД.9	Ограничение числа параллельных сеансов доступа			+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+
УПД.12	Управление атрибутами безопасности			
УПД.13	Реализация защищенного удаленного доступа	+	+	+
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+
III. Ограничение программной среды (ОПС)				
ОПС.0	Разработка политики ограничения программной среды		+	+
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+
ОПС.3	Управление временными файлами			
IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.0	Разработка политики защиты машинных носителей информации	+	+	+
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+	+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			+

ЗНИ.7	Контроль подключения машинных носителей информации	+	+	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+	+	+
V. Аудит безопасности (АУД)				
АУД.0	Разработка политики аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+
VI. Антивирусная защита (АВЗ)				
АВЗ.0	Разработка политики антивирусной защиты	+	+	+
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
АВЗ.5	Использование средств антивирусной защиты различных производителей			+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+

VIII. Обеспечение целостности (ОЦЛ)				
ОЦЛ.0	Разработка политики обеспечения целостности	+	+	+
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+
ОЦЛ.2	Контроль целостности информации			
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+
ОЦЛ.6	Обезличивание и (или) деидентификация информации			
IX. Обеспечение доступности (ОДТ)				
ОДТ.0	Разработка политики обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
ОДТ.2	Резервирование средств и систем		+	+
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+
ОДТ.4	Резервное копирование информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+
ОДТ.7	Кластеризация информационной (автоматизированной) системы			
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+
X. Защита технических средств и систем (ЗТС)				
ЗТС.0	Разработка политики защиты технических средств и систем	+	+	+
ЗТС.1	Защита информации от утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны	+	+	+
ЗТС.3	Управление физическим доступом	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+
ЗТС.5	Защита от внешних воздействий	+	+	+
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации			

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+	+	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками			
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения («песочница»)			
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+
ЗИС.9	Создание гетерогенной среды			
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем			
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.13	Защита неизменяемых данных		+	+
ЗИС.14	Использование неперезаписываемых машинных носителей информации			
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек			
ЗИС.16	Защита от спама		+	+
ЗИС.17	Защита информации от утечек			
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию			
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+	+	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+

ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами			
ЗИС.23	Контроль использования мобильного кода		+	+
ЗИС.24	Контроль передачи речевой информации		+	+
ЗИС.25	Контроль передачи видеоинформации		+	+
ЗИС.26	Подтверждение происхождения источника информации			
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+
ЗИС.28	Исключение возможности отрицания отправки информации		+	+
ЗИС.29	Исключение возможности отрицания получения информации		+	+
ЗИС.30	Использование устройств терминального доступа			
ЗИС.31	Защита от скрытых каналов передачи информации			+
ЗИС.32	Защита беспроводных соединений	+	+	+
ЗИС.33	Исключение доступа через общие ресурсы			+
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	+	+
ЗИС.35	Управление сетевыми соединениями		+	+
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем			
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)			
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+
XII. Реагирование на компьютерные инциденты (ИНЦ)				
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+	+	+
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах			+

XIII. Управление конфигурацией (УКФ)				
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	+	+	+
УКФ.1	Идентификация объектов управления конфигурацией			
УКФ.2	Управление изменениями	+	+	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			
XIV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Разработка политики управления обновлениями программного обеспечения	+	+	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)				
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	+	+	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+	+	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+	+	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+	+	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+

ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+	+	+
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+
XVII. Информирование и обучение персонала (ИПО)				
ИПО.0	Разработка политики информирования и обучения персонала	+	+	+
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+

«+» – мера защиты информации включена в базовый набор мер для соответствующего класса защищенности автоматизированной системы управления.

Меры защиты информации, не обозначенные знаком «+», применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер защиты информации в автоматизированной системе управления соответствующего класса защищенности.».

2. В приложении к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239, строку седьмую раздела XVI изложить в следующей редакции:

«	ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+ »