Приказ ФСТЭК России от 14.03.2014 № 31 "Об утверждении Требований 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"

(в ред. Приказов ФСТЭК России от 23.03.2017 № 49, от 09.08.2018 № 138)

Зарегистрировано в Минюсте России 30 июня 2014 г. № 32919

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным 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), приказываю:

Утвердить прилагаемые 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.

Директор
Федеральной службы по техническому
и экспортному контролю
В.Селин

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

Утверждены
приказом ФСТЭК России
от 14 марта 2014 г. № 31

I. Общие положения

1. В настоящем документе устанавливаются требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (далее - автоматизированные системы управления), от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

Настоящие Требования применяются в случае принятия владельцем автоматизированной системы управления решения об обеспечении защиты информации, обработка которой осуществляется этой системой и нарушение безопасности которой может привести к нарушению функционирования автоматизированной системы управления.

В случае необходимости применение криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

2. Настоящие Требования направлены на обеспечение функционирования автоматизированной системы управления в штатном режиме, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения целевых функций автоматизированной системы управления в условиях воздействия угроз безопасности информации, а также на снижение рисков незаконного вмешательства в процессы функционирования автоматизированных систем управления критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов (далее - управляемые (контролируемые) объекты), безопасность которых обеспечивается в соответствии с законодательством Российской Федерации о безопасности объектов топливно-энергетического комплекса, о транспортной безопасности, об использовании атомной энергии, о промышленной безопасности опасных производственных объектов, о безопасности гидротехнических сооружений и иных законодательных актов Российской Федерации.

3. Действие настоящих требований распространяется на автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).

4. Настоящие Требования предназначены для лиц, устанавливающих требования к защите информации в автоматизированных системах управления (далее - заказчик), лиц, обеспечивающих эксплуатацию автоматизированных систем управления (далее - оператор), а также лиц, привлекаемых в соответствии с законодательством Российской Федерации к проведению работ по созданию (проектированию) автоматизированных систем управления и (или) их систем защиты (далее - разработчик).

5. При обработке в автоматизированной системе управления информации, составляющей государственную тайну, ее защита обеспечивается в соответствии с законодательством Российской Федерации о государственной тайне.

6. Защита информации в автоматизированной системе управления обеспечивается путем выполнения заказчиком, оператором и разработчиком требований к организации защиты информации в автоматизированной системе управления и требований к мерам защиты информации в автоматизированной системе управления.

II. Требования к организации защиты информации в автоматизированной системе управления

7. Автоматизированная система управления, как правило, имеет многоуровневую структуру:
уровень операторского (диспетчерского) управления (верхний уровень);
уровень автоматического управления (средний уровень);
уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень). Автоматизированная система управления может включать:
а) на уровне операторского (диспетчерского) управления:
операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи;
б) на уровне автоматического управления:
программируемые логические контроллеры, иные технические средства с установленным программным обеспечением, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды (управляющую (командную) информацию) для исполнительных устройств, а также промышленная сеть передачи данных;
в) на уровне ввода (вывода) данных (исполнительных устройств):
датчики, исполнительные механизмы, иные аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

Количество уровней автоматизированной системы управления и ее состав на каждом из уровней зависит от назначения автоматизированной системы управления и выполняемых ею целевых функций. На каждом уровне автоматизированной системы управления по функциональным, территориальным или иным признакам могут выделяться дополнительные сегменты.

В автоматизированной системе управления объектами защиты являются:
информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);
программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации.

8. Защита информации в автоматизированной системе управления является составной частью работ по созданию (модернизации) и эксплуатации автоматизированной системы управления и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации.

Защита информации в автоматизированной системе управления достигается путем принятия в рамках системы защиты автоматизированной системы управления совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

Принимаемые организационные и технические меры защиты информации:
должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);
должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными

мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса;
не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

9. Проведение работ по защите информации в соответствии с настоящими Требованиями в ходе создания (модернизации) и эксплуатации автоматизированной системы управления осуществляется заказчиком, оператором и (или) разработчиком самостоятельно и (или) при необходимости с привлечением в соответствии с законодательством Российской Федерации организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2011, № 19, ст. 2716; № 30, ст. 4590; № 43, ст. 5971; № 48, ст. 6728; 2012, № 26, ст. 3446; № 31, ст. 4322; 2013, № 9, ст. 874; № 27, ст. 3477).

10. Для обеспечения защиты информации в автоматизированной системе управления оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

11. В автоматизированной системе управления применяются средства защиты информации, прошедшие оценку соответствия в соответствии с законодательством Российской Федерации о техническом регулировании.

12. Для обеспечения защиты информации в автоматизированной системе управления проводятся следующие мероприятия:
формирование требований к защите информации в автоматизированной системе управления;
разработка системы защиты автоматизированной системы управления;
внедрение системы защиты автоматизированной системы управления и ввод ее в действие;
обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;
обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.

Формирование требований к защите информации в автоматизированной системе управления

13. Формирование требований к защите информации в автоматизированной системе управления осуществляется заказчиком.

Формирование требований к защите информации в автоматизированной системе управления осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583), ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и стандартов организации и в том числе включает:
принятие решения о необходимости защиты информации в автоматизированной системе управления;
классификацию автоматизированной системы управления по требованиям защиты информации (далее - классификация автоматизированной системы управления);
определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления, и разработку на их основе модели угроз безопасности информации;
определение требований к системе защиты автоматизированной системы управления.

13.1. При принятии решения о необходимости защиты информации в автоматизированной системе управления осуществляются:
анализ целей создания автоматизированной системы управления и задач, решаемых этой автоматизированной системой управления;
определение информации, нарушение доступности, целостности или конфиденциальности которой может привести к нарушению штатного режима функционирования автоматизированной системы управления (определение критически важной информации), и оценка возможных последствий такого нарушения;
анализ нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления;
принятие решения о необходимости создания системы защиты автоматизированной системы управления и определение целей и задач защиты информации в автоматизированной системе управления.

13.2. Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.

Устанавливаются три класса защищенности автоматизированной системы управления, определяющие уровни защищенности автоматизированной системы управления. Самый низкий класс - третий, самый высокий - первый. Класс защищенности автоматизированной системы управления определяется в соответствии с приложением № 1 к настоящим Требованиям.

Класс защищенности может быть установлен отдельно для каждого из уровней автоматизированной системы управления или иных сегментов при их наличии.

Результаты классификации автоматизированной системы управления оформляются актом классификации.

Требование к классу защищенности включается в техническое задание на создание автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее - ГОСТ 34.602), ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации.

Класс защищенности автоматизированной системы управления (сегмента) подлежит пересмотру только в случае ее модернизации,

в результате которой изменился уровень значимости (критичности) информации, обрабатываемой в автоматизированной системе управления (сегменте). 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.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики автоматизированной системы управления, включающие наличие уровней (сегментов) автоматизированной системы управления, состав автоматизированной системы управления, физические, логические, функциональные и технологические взаимосвязи в автоматизированной системе управления, взаимодействие с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, режимы функционирования автоматизированной системы управления, а также иные особенности ее построения и функционирования.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурно-функциональных характеристик автоматизированной системы управления, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание автоматизированной системы управления и угроз безопасности информации для каждого из уровней автоматизированной системы управления, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования автоматизированной системы управления[1)].

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России[2)].

13.4. Требования к системе защиты автоматизированной системы управления определяются в зависимости от класса защищенности автоматизированной системы управления и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты автоматизированной системы управления включаются в техническое задание на создание (модернизацию) автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации, которые должны в том числе содержать:
цель и задачи обеспечения защиты информации в автоматизированной системе управления;
класс защищенности автоматизированной системы управления;
перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления;
объекты защиты автоматизированной системы управления на каждом из ее уровней;
требования к мерам и средствам защиты информации, применяемым в автоматизированной системе управления;
требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;
требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
функции заказчика и оператора по обеспечению защиты информации в автоматизированной системе управления;
стадии (этапы работ) создания системы защиты автоматизированной системы управления.

При определении требований к системе защиты автоматизированной системы управления учитываются положения политик обеспечения информационной безопасности заказчика в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», а также политик обеспечения информационной безопасности оператора в части, не противоречащей политикам заказчика.

Разработка системы защиты автоматизированной системы управления

14. Разработка системы защиты автоматизированной системы управления организуется заказчиком и осуществляется разработчиком и (или) оператором.

Разработка системы защиты автоматизированной системы управления осуществляется в соответствии с техническим заданием на создание (модернизацию) автоматизированной системы управления и (или) техническим заданием (частным техническим заданием) на создание системы защиты автоматизированной системы управления с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации и в том числе включает:
проектирование системы защиты автоматизированной системы управления;
разработку эксплуатационной документации на систему защиты автоматизированной системы управления.

Система защиты автоматизированной системы управления не должна препятствовать штатному режиму функционирования автоматизированной системы управления при выполнении ее функций в соответствии с назначением автоматизированной системы управления.

При разработке системы защиты автоматизированной системы управления учитывается ее информационное взаимодействие с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями.

14.1. При проектировании системы защиты автоматизированной системы управления:
определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа);
определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления;
выбираются меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления;
определяются параметры программирования и настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей автоматизированной системы управления;
определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
определяется структура системы защиты автоматизированной системы управления, включая состав (количество) и места размещения ее элементов;
осуществляется при необходимости выбор средств защиты информации с учетом их стоимости, совместимости с программным обеспечением и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности автоматизированной системы управления;
определяются меры защиты информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;
осуществляется проверка, в том числе при необходимости с использованием макетов или тестовой зоны, корректности функционирования автоматизированной системы управления с системой защиты и совместимости выбранных средств защиты информации с программным обеспечением и техническими средствами автоматизированной системы управления.

При проектировании системы защиты автоматизированной системы управления должны учитываться особенности функционирования программного обеспечения и технических средств на каждом из уровней автоматизированной системы управления.

Результаты проектирования системы защиты автоматизированной системы управления отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на автоматизированную систему управления (систему защиты автоматизированной системы управления), разрабатываемой с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее - ГОСТ 34.201) и стандартов организации.

14.2. Разработка эксплуатационной документации на систему защиты автоматизированной системы управления осуществляется по результатам проектирования в соответствии с техническим заданием на создание (модернизацию) автоматизированной системы управления и (или) техническим заданием (частным техническим заданием) на создание системы защиты автоматизированной системы управления.

Эксплуатационная документация на систему защиты автоматизированной системы управления разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201, ГОСТ Р 51624 и стандартов организации и должна в том числе содержать описание:
структуры системы защиты автоматизированной системы управления;
состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
правил эксплуатации системы защиты автоматизированной системы управления.

Внедрение системы защиты автоматизированной системы управления и ввод ее в действие

15. Внедрение системы защиты автоматизированной системы управления организуется заказчиком и осуществляется разработчиком и (или) оператором.

Внедрение системы защиты автоматизированной системы управления осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации автоматизированной системы управления и в том числе включает:

настройку (задание параметров программирования) программного обеспечения автоматизированной системы управления;
разработку документов, определяющих правила и процедуры (политики), реализуемые оператором для обеспечения защиты информации в автоматизированной системе управления в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);
внедрение организационных мер защиты информации;
установку и настройку средств защиты информации в автоматизированной системе управления;
предварительные испытания системы защиты автоматизированной системы управления;
опытную эксплуатацию системы защиты автоматизированной системы управления;
анализ уязвимостей автоматизированной системы управления и принятие мер по их устранению;
приемочные испытания системы защиты автоматизированной системы управления.

15.1. Настройка (задание параметров программирования) программного обеспечения автоматизированной системы управления должна осуществляться в соответствии с проектной и эксплуатационной документацией на автоматизированную систему управления и обеспечивать конфигурацию программного обеспечения и автоматизированной системы в целом, при которой минимизируются риски возникновения уязвимостей и возможности реализации угроз безопасности информации.

15.2. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры (политики):
реализаций отдельных мер защиты информации в автоматизированной системе управления в рамках ее системы защиты;
планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления;
обеспечения действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;
информирования и обучения персонала автоматизированной системы управления;
анализа угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;
управления (администрирования) системой защиты информации автоматизированной системы управления;
выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования автоматизированной системы управления и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
управления конфигурацией автоматизированной системы управления и ее системы защиты;
контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;
защиты информации при выводе из эксплуатации автоматизированной системы управления.

Организационно-распорядительные документы по защите информации могут разрабатываться в виде отдельных документов оператора или в рамках общей политики обеспечения информационной безопасности в случае ее разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

15.3. При внедрении организационных мер защиты информации осуществляются:
введение ограничений на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации технических средств и программного обеспечения;
определение администратора безопасности информации;
реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа;
проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий персонала автоматизированной системы управления и администратора безопасности информации, направленных на обеспечение защиты информации;
отработка практических действий должностных лиц и подразделений, обеспечивающих эксплуатацию автоматизированной системы управления и защиту информации.

15.4. Установка и настройка средств защиты информации осуществляется в случаях, если такие средства необходимы для блокирования (нейтрализации) угроз безопасности информации, которые невозможно исключить настройкой (заданием параметров) программного обеспечения автоматизированной системы управления и (или) реализацией организационных мер защиты информации.

Установка и настройка средств защиты информации в автоматизированной системе управления должна проводиться в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и документацией на средства защиты информации.

При этом установка и настройка средств защиты информации должна обеспечивать корректность функционирования автоматизированной системы управления и совместимость выбранных средств защиты информации с программным обеспечением и техническими средствами автоматизированной системы управления. Установленные и настроенные средства защиты информации не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

15.5. Предварительные испытания системы защиты автоматизированной системы управления проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» (далее - ГОСТ 34.603) и стандартов организации и включают проверку работоспособности системы защиты автоматизированной системы управления, а также принятие решения о возможности опытной эксплуатации системы защиты автоматизированной системы управления.

По результатам предварительных испытаний системы защиты автоматизированной системы управления могут разрабатываться предложения по корректировке проектных решений по автоматизированной системе управления и (или) ее системе защиты.

15.6. Опытная эксплуатация системы защиты автоматизированной системы управления проводится с учетом ГОСТ 34.603 и

стандартов организации и включает проверку функционирования системы защиты автоматизированной системы управления, в том числе реализованных мер защиты информации, а также готовность персонала автоматизированной системы управления к эксплуатации системы защиты автоматизированной системы управления.

По результатам опытной эксплуатации системы защиты автоматизированной системы управления могут разрабатываться предложения по корректировке проектных решений по автоматизированной системе управления и (или) ее системе защиты.

15.7. Анализ уязвимостей автоматизированной системы управления проводится в целях оценки возможности преодоления нарушителем системы защиты автоматизированной системы управления и нарушения безопасного функционирования автоматизированной системы управления за счет реализации угроз безопасности информации.

Анализ уязвимостей автоматизированной системы управления включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения автоматизированной системы управления.

При анализе уязвимостей автоматизированной системы управления проверяется отсутствие уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации, технических средств и программного обеспечения автоматизированной системы управления при их взаимодействии.

По решению заказчика для подтверждения выявленных уязвимостей может проводиться тестирование автоматизированной системы управления на проникновение. Указанное тестирование проводится, как правило, на макете (в тестовой зоне) автоматизированной системы управления.

В случае выявления уязвимостей в автоматизированной системе управления, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность эксплуатации нарушителем выявленных уязвимостей.

Анализ уязвимостей автоматизированной системы управления проводится до ввода автоматизированной системы управления в промышленную эксплуатацию на этапах, определяемых заказчиком.

15.8. Приемочные испытания системы защиты автоматизированной системы управления проводятся, как правило, в рамках приемочных испытаний автоматизированной системы управления в целом с учетом ГОСТ 34.603 и стандартов организации.

В ходе приемочных испытаний должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие системы защиты автоматизированной системы управления техническому заданию на создание (модернизацию) автоматизированной системы управления и (или) техническому заданию (частному техническому заданию) на создание системы защиты автоматизированной системы управления, а также настоящим Требованиям.

В качестве исходных данных при приемочных испытаниях используются модель угроз безопасности информации, акт классификации автоматизированной системы управления, техническое задание на создание (модернизацию) автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, проектная и эксплуатационная документация на систему защиты автоматизированной системы управления, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей автоматизированной системы управления, материалы предварительных и приемочных испытаний системы защиты автоматизированной системы управления, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями и требованиями стандартов организации.

Приемочные испытания системы защиты автоматизированной системы управления проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний системы защиты автоматизированной системы управления с выводом о ее соответствии установленным требованиям включаются в акт приемки автоматизированной системы управления в эксплуатацию.

По решению заказчика подтверждение соответствия системы защиты автоматизированной системы управления техническому заданию на создание (модернизацию) автоматизированной системы управления и (или) техническому заданию (частному техническому заданию) на создание системы защиты автоматизированной системы управления, а также настоящим Требованиям может проводиться в форме аттестации автоматизированной системы управления на соответствие требованиям по защите информации. В этом случае для проведения аттестации применяются национальные стандарты, а также методические документы ФСТЭК России[3)].

Ввод в действие автоматизированной системы управления осуществляется с учетом ГОСТ 34.601, стандартов организации и при положительном заключении (выводе) в акте приемки о соответствии ее системы защиты установленным требованиям к защите информации (или при наличии аттестата соответствия).

Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления

16. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты и организационно-распорядительными документами по защите информации и включает следующие процедуры:

планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления;
обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;
информирование и обучение персонала автоматизированной системы управления;
периодический анализ угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;
управление (администрирование) системой защиты автоматизированной системы управления;
выявление инцидентов в ходе эксплуатации автоматизированной системы управления и реагирование на них;
управление конфигурацией автоматизированной системы управления и ее системы защиты;
контроль (мониторинг) за обеспечением уровня защищенности автоматизированной системы управления.

16.1. В ходе планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления осуществляются:
определение лиц, ответственных за планирование и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления;
разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированной системе управления;
контроль выполнения мероприятий по обеспечению защиты информации в автоматизированной системе управления, предусмотренных утвержденным планом.

16.2. В ходе обеспечения действий в нештатных (непредвиденных) ситуациях при эксплуатации автоматизированной системы управления осуществляются:
планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления на случай возникновения нештатных (непредвиденных) ситуаций;
обучение и отработка действий персонала по обеспечению защиты информации в автоматизированной системе управления в случае возникновения нештатных (непредвиденных) ситуаций;
создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций;
резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных (непредвиденных) ситуаций;
обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонентов в случае возникновения нештатных (непредвиденных) ситуаций.

16.3. В ходе информирования и обучения персонала автоматизированной системы управления осуществляются:
периодическое информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации;
периодическое обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.

16.4. В ходе анализа угроз безопасности информации в автоматизированной системе управления и возможных рисков от их реализации осуществляются:
периодический анализ уязвимостей автоматизированной системы управления, возникающих в ходе ее эксплуатации;
периодический анализ изменения угроз безопасности информации в автоматизированной системе управления, возникающих в ходе ее эксплуатации;
периодическая оценка последствий от реализации угроз безопасности информации в автоматизированной системе управления (анализ риска).

16.5. В ходе управления (администрирования) системой защиты автоматизированной системы управления осуществляются:
определение лиц, ответственных за управление (администрирование) системой защиты автоматизированной системы управления;
управление учетными записями пользователей и поддержание правил разграничения доступа в автоматизированной системе управления в актуальном состоянии;
управление средствами защиты информации в автоматизированной системе управления, в том числе параметрами настройки программного обеспечения, включая восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
управление обновлениями программного обеспечения, включая программное обеспечение средств защиты информации, с учетом особенностей функционирования автоматизированной системы управления;
централизованное управление системой защиты автоматизированной системы управления (при необходимости);
анализ зарегистрированных событий в автоматизированной системе управления, связанных с безопасностью информации (далее - события безопасности);
сопровождение функционирования системы защиты автоматизированной системы управления в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

16.6. Для выявления инцидентов и реагирования на них осуществляются:
определение лиц, ответственных за выявление инцидентов и реагирование на них;
обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в автоматизированной системе управления персоналом;
анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
планирование и принятие мер по устранению инцидентов, в том числе по восстановлению автоматизированной системы управления в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа,

неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
планирование и принятие мер по предотвращению повторного возникновения инцидентов.

16.7. В ходе управления конфигурацией автоматизированной системы управления и ее системы защиты осуществляются:
поддержание конфигурации автоматизированной системы управления и ее системы защиты (структуры системы защиты автоматизированной системы управления, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты (поддержание базовой конфигурации автоматизированной системы управления и ее системы защиты);
определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;
регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления;
управление изменениями базовой конфигурации автоматизированной системы управления и ее системы защиты, в том числе определение типов возможных изменений базовой конфигурации автоматизированной системы управления и ее системы защиты, санкционирование внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, документирование действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, сохранение данных об изменениях базовой конфигурации автоматизированной системы управления и ее системы защиты, контроль действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;
анализ потенциального воздействия планируемых изменений в базовой конфигурации автоматизированной системы управления и ее системы защиты на обеспечение ее безопасности, возникновение дополнительных угроз безопасности информации и работоспособность автоматизированной системы управления;
определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;
внесение информации (данных) об изменениях в базовой конфигурации автоматизированной системы управления и ее системы защиты в эксплуатационную документацию на систему защиты информации автоматизированной системы управления.

16.8. В ходе контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления осуществляются:
контроль за событиями безопасности и действиями персонала в автоматизированной системе управления;
контроль (анализ) защищенности информации, обрабатываемой в автоматизированной системе управления, с учетом особенностей ее функционирования;
анализ и оценка функционирования системы защиты автоматизированной системы управления, включая выявление, анализ и устранение недостатков в функционировании системы защиты автоматизированной системы управления;
документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;
принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления о необходимости пересмотра требований к защите информации в автоматизированной системе управления и доработке (модернизации) ее системы защиты.

Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления

17. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и организационно-распорядительными документами по защите информации и в том числе включает:
архивирование информации, содержащейся в автоматизированной системе управления;
уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

17.1. Архивирование информации, содержащейся в автоматизированной системе управления, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

17.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю автоматизированной системы управления или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе автоматизированной системы управления из эксплуатации производится уничтожение машинных носителей информации, содержащих энергонезависимую память.

III. Требования к мерам защиты информации в автоматизированной системе управления

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.

18.1 - 18.21. Утратили силу. - Приказ ФСТЭК России от 09.08.2018 № 138.

19. Выбор мер защиты информации для их реализации в автоматизированной системе управления в рамках ее системы защиты включает:
определение базового набора мер защиты информации для установленного класса защищенности автоматизированной системы управления в соответствии с базовыми наборами мер защиты информации, приведенными в приложении № 2 к настоящим Требованиям;
адаптацию базового набора мер защиты информации применительно к каждому уровню автоматизированной системы управления, иным структурно-функциональным характеристикам и особенностям функционирования автоматизированной системы управления (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с технологиями, не используемыми в автоматизированной системе управления или ее уровнях, или структурно-функциональными характеристиками, не свойственными автоматизированной системе управления);
уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении № 2 к настоящим Требованиям, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации на каждом из уровней автоматизированной системы управления;
дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленными иными нормативными правовыми актами, локальными правовыми актами, национальными стандартами и стандартами организации в области защиты информации.

Для выбора мер защиты информации для соответствующего класса защищенности автоматизированной системы управления применяются методические документы ФСТЭК России[4)].

20. В автоматизированной системе управления соответствующего класса защищенности в рамках ее системы защиты должны быть реализованы меры защиты информации, выбранные в соответствии с пунктами 18 и 19 настоящих Требований и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации на каждом из уровней автоматизированной системы управления.

Выбранные меры защиты информации рассматриваются для каждого уровня автоматизированной системы управления отдельно и подлежат реализации с учетом особенностей функционирования каждого из уровней.

При этом в автоматизированной системе управления должен быть, как минимум, реализован адаптированный для каждого уровня базовый набор мер защиты информации, соответствующий установленному классу защищенности автоматизированной системы управления.

21. В целях исключения избыточности в реализации мер защиты информации и в случае, если принятые в автоматизированной системе управления меры по обеспечению промышленной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры защиты информации, выбранные в соответствии с пунктами 18 и 19 настоящих Требований, могут не применяться. При этом в ходе разработки системы защиты автоматизированной системы управления должно быть проведено обоснование достаточности применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации.

22. При отсутствии возможности реализации отдельных мер защиты информации на каком-либо из уровней автоматизированной системы управления и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на штатный режим функционирования автоматизированной системы управления, на этапах адаптации

базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации разрабатываются иные (компенсирующие) меры, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации и необходимый уровень защищенности автоматизированной системы управления.

В качестве компенсирующих мер, в первую очередь, рассматриваются меры по обеспечению промышленной и (или) физической безопасности автоматизированной системы управления, поддерживающие необходимый уровень защищенности автоматизированной системы управления.

В этом случае в ходе разработки системы защиты автоматизированной системы управления должно быть проведено обоснование применения компенсирующих мер, а при приемочных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

23. Выбранные и реализованные в автоматизированной системе управления в рамках ее системы защиты меры защиты информации, как минимум, должны обеспечивать:
в автоматизированных системах управления 1 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;
в автоматизированных системах управления 2 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с потенциалом не ниже среднего;
в автоматизированных системах управления 3 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом.

Потенциал нарушителя определяется в ходе оценки его возможностей и мотивации, проводимой при анализе угроз безопасности информации в соответствии с пунктом 13.3 настоящих Требований.

Оператором может быть принято решение о применении в автоматизированной системе управления соответствующего класса защищенности мер защиты информации, обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителем с более высоким потенциалом.

24. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления при их наличии.

В случае использования в автоматизированных системах управления сертифицированных по требованиям безопасности информации средств защиты информации применяются:
в автоматизированных системах управления 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;
в автоматизированных системах управления 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;
в автоматизированных системах управления 3 класса защищенности применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В случае использования в автоматизированных системах управления средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.

В автоматизированных системах управления 1 и 2 классов защищенности применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Заказчиком (оператором) в зависимости от потенциала нарушителя может быть принято решение о повышении уровня контроля отсутствия недекларированных возможностей средств защиты информации.

25. При использовании в автоматизированных системах управления новых технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры защиты информации, должны разрабатываться компенсирующие меры в соответствии с пунктом 22 настоящих Требований.

Приложение № 1 к Требованиям

Определение класса защищенности автоматизированной системы управления

Приложение № 2 к Требованиям

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

безопасность критической информационной инфраструктуры, аттестация

[1] , [2] Разработанные ФСТЭК России в соответствии с подпунктом 4 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).

[3] , [4] Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.