Зарегистрировано в Минюсте России 30 июня 2014 г. N 32919

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 14 марта 2014 г. N 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

Список изменяющих документов
(в ред. Приказов ФСТЭК России от 23.03.2017 N 49,
от 09.08.2018 N 138)

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 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

Утверждены
приказом ФСТЭК России
от 14 марта 2014 г. N 31

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

Список изменяющих документов
(в ред. Приказов ФСТЭК России от 23.03.2017 N 49,
от 09.08.2018 N 138)

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.

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. N 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. N 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный N 50118).
(абзац введен Приказом ФСТЭК России от 09.08.2018 N 138)

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. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874; N 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 N 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:
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

б) анализ возможных уязвимостей автоматизированной системы и входящих в ее состав программных и программно-аппаратных средств;
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

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 ред. Приказа ФСТЭК России от 09.08.2018 N 138)

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. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; N 4, ст. 641; 2016, N 1, ст. 211; 2017, N 48, ст. 7198; 2018, N 20, ст. 2818), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

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 <*>.

<*> 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. N 1085 (Собрание законодательства

Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137).

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России <*>.

<*> 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. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137).

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;
(абзац введен Приказом ФСТЭК России от 09.08.2018 N 138)

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;
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

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 <*>.

<*> 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. N 1085.

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 N 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. N 1085.
(п. 18 в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

18.1 - 18.21. Утратили силу. - Приказ ФСТЭК России от 09.08.2018 N 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 N 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 N 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 <*>.

<*> 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. N 1085.

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. N 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.
(п. 24 в ред. Приказа ФСТЭК России от 23.03.2017 N 49)

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 N 1
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

ОПРЕДЕЛЕНИЕ
КЛАССА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

1. Класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

2. Уровень значимости (критичности) информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется заказчиком или оператором экспертным или иным методом и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации федерального или межрегионального характера <*> или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера <*> или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации муниципального (локального) <*> характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

В случае, если для информации, обрабатываемой в автоматизированной системе управления, не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности) уровень значимости (критичности) определятся для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

Информация, обрабатываемая в автоматизированной системе управления, имеет высокий уровень значимости (критичности) (УЗ 1), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет средний уровень значимости (критичности) (УЗ 2), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет низкий уровень значимости (критичности) (УЗ 3), если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

При обработке в автоматизированной системе управления двух и более видов информации (измерительная информация, информация о состоянии процесса) уровень значимости (критичности) информации (УЗ) определяется отдельно для каждого вида информации. Итоговый уровень значимости (критичности) устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

3. Класс защищенности автоматизированной системы управления определяется в соответствии с таблицей:

Уровень значимости (критичности) информации	Класс защищенности автоматизированной системы управления
УЗ 1	К1
УЗ 2	К2
УЗ 3	К3

Приложение N 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

Список изменяющих документов
(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

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.