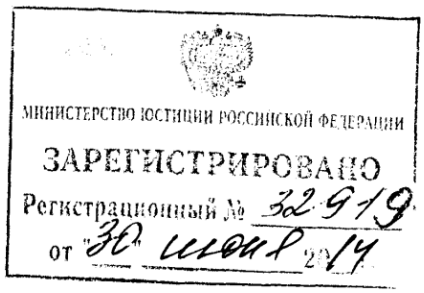

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«14» марта 2014 г. Москва № 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 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),
П Р И К А З Ы В А Ю:

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. № 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

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. Угрозы безопасности информации определяются на каждом из уровней автоматизированной системы управления по результатам:

оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей;

анализа возможных уязвимостей автоматизированной системы управления;

анализа возможных способов (сценариев) реализации угроз безопасности информации и последствий от нарушения как отдельных свойств безопасности информации (целостности, доступности, конфиденциальности), так и автоматизированной системы управления в целом.

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.*

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

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

---

* 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).

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), разрабатываемых 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):

реализации 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;

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, 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*.

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.

---

* 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.

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 субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

целостность автоматизированной системы управления и информации;

доступность технических средств и информации;

защиту среды виртуализации;

защиту технических средств и оборудования;

защиту автоматизированной системы и ее компонентов;

безопасную разработку прикладного и специального программного обеспечения;

управление обновлениями программного обеспечения;

планирование мероприятий по обеспечению защиты информации;

обеспечение действий в нештатных (непредвиденных) ситуациях;

информирование и обучение персонала;

анализ угроз безопасности информации и рисков от их реализации;

выявление инцидентов и реагирование на них (управление инцидентами);

управление конфигурацией автоматизированной системы управления и ее системы защиты.

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

18.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

18.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в автоматизированной системе управления правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

18.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в автоматизированной системе управления программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в автоматизированной системе управления программного обеспечения.

18.4. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

18.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в автоматизированной системе управления, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

18.6. Меры по антивирусной защите должны обеспечивать обнаружение в автоматизированной системе управления компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

18.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в автоматизированной системе управления, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на автоматизированную систему управления и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

18.8. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности автоматизированной системы управления путем проведения мероприятий по выявлению и анализу уязвимостей, контролю установки обновлений программного обеспечения, состава программного обеспечения и технических средств и правильности функционирования средств защиты информации.

18.9. Меры по обеспечению целостности автоматизированной системы управления и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности автоматизированной системы управления и содержащихся в ней данных, а также возможность восстановления автоматизированной системы управления.

18.10. Меры по обеспечению доступности технических средств и информации должны обеспечивать авторизованный доступ персонала, имеющего права по такому доступу к техническим средствам (исполнительным устройствам) и информации, а также доступность технических средств (исполнительных устройств) для входной (выходной) информации, управляющей (командной) информации, контрольно-измерительной информации, иной критически важной информации в штатном режиме функционирования автоматизированной системы управления.

18.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

18.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, исполнительным устройствам, средствам, обеспечивающим функционирование автоматизированной системы управления (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивать защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

18.13. Меры по защите автоматизированной системы и ее компонентов должны обеспечивать защиту информации при ее передаче по каналам связи,

взаимодействии автоматизированной системы управления или ее отдельных сегментов с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями посредством применения архитектуры автоматизированной системы управления и проектных решений по ее системе защиты, направленных на обеспечение защиты информации.

18.14. Меры по обеспечению безопасной разработки прикладного и специального программного обеспечения должны обеспечивать выявление, анализ и устранение разработчиком уязвимостей программного обеспечения автоматизированной системы управления, определенного заказчиком, на всех этапах (стадиях) его разработки, а также контроль принимаемых мер по выявлению, анализу и устранению уязвимостей со стороны заказчика и (или) оператора автоматизированной системы управления.

18.15. Меры по управлению обновлениями программного обеспечения должны обеспечивать безопасное получение, проверку и установку обновлений программного обеспечения на компонентах автоматизированной системы управления технологическими процессами.

18.16. Меры по планированию мероприятий по обеспечению защиты информации должны обеспечивать разработку, утверждение и актуализацию плана мероприятий по обеспечению защиты информации в автоматизированных системах управления, в том числе предусматривающего мероприятия по защите информации в ходе создания, эксплуатации и вывода из эксплуатации автоматизированной системы управления, сроки выполнения мероприятий и ответственных за их выполнение, а также контроль его выполнения.

18.17. Меры по обеспечению действий в нештатных (непредвиденных) ситуациях должны обеспечивать планирование мероприятий, обучение и отработку действий персонала в случае возникновения нештатных (непредвиденных) ситуаций, а также резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления в случае возникновения нештатных (непредвиденных) ситуаций и обеспечение возможности ее восстановления.

18.18. Меры по информированию и обучению персонала должны обеспечивать информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации, а также теоретическое и практическое обучение (в том числе проведение тренировок) по эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации.

18.19. Меры по анализу угроз безопасности информации и рисков от их реализации должны обеспечивать периодический анализ изменения угроз безопасности информации в автоматизированной системе управления, возникающих в ходе ее эксплуатации, а также периодическую оценку (переоценку) прогнозируемых последствий от реализации угроз безопасности информации в автоматизированной системе управления.

18.20. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в

автоматизированной системе управления, а также принятие мер по устранению и предупреждению инцидентов.

18.21. Меры по управлению конфигурацией автоматизированной системы управления и ее системы защиты информации должны обеспечивать управление изменениями конфигурации автоматизированной системы управления и ее системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений.

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*.

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

---

*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.

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, 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:

а) в автоматизированных системах управления 1 класса защищенности:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 3 класса;

межсетевые экраны не ниже 3 класса в случае взаимодействия автоматизированной системы управления с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

б) в автоматизированных системах управления 2 класса защищенности:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае взаимодействия автоматизированной системы управления с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

в) в автоматизированных системах управления 3 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 5 класса;

межсетевые экраны не ниже 4 класса.

В случае использования сертифицированных средств защиты информации в автоматизированной системе управления 1 и 2 классов защищенности применяются 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 в программном обеспечении 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 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;

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;

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.

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.

---

* Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера» (Собрание законодательства Российской Федерации, 2007, № 22, ст. 2640; 2011, № 21, ст. 2971).

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

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

Условное обозначение и номер меры	Меры защиты информации в автоматизированных системах управления	Классы защищенности		
		3	2	1
1	2	3	4	5
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.0	Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5	Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+

1	2	3	4	5
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа			
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.0	Разработка правил и процедур (политик) управления доступом субъектов доступа к объектам доступа	+	+	+
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+
УПД.3	Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование автоматизированной системы управления	+	+	+
УПД.6	Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе)	+	+	+
УПД.7	Предупреждение пользователя при его входе в автоматизированную систему управления о том, что в ней реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации			
УПД.8	Оповещение пользователя после успешного входа в автоматизированную систему управления о его предыдущем входе в автоматизированную систему управления			
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя автоматизированной системы управления			

1	2	3	4	5
УПД.10	Блокирование сеанса доступа в автоматизированную систему управления после установленного времени бездействия (неактивности) пользователя или по его запросу			
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+
УПД.14	Регламентация и контроль использования в автоматизированной системе управления технологий беспроводного доступа	+	+	+
УПД.15	Регламентация и контроль использования в автоматизированной системе управления мобильных технических средств	+	+	+
УПД.16	Управление взаимодействием с автоматизированными (информационными) системами сторонних организаций (внешние системы)	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			
III. Ограничение программной среды (ОПС)				
ОПС.0	Разработка правил и процедур (политик) ограничения программной среды	+	+	+
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			
IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.0	Разработка правил и процедур (политик) защиты машинных носителей	+	+	+

1	2	3	4	5
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных автоматизированных системах управления			
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 при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)			
V. Регистрация событий безопасности (РСБ)				
РСБ.0	Разработка правил и процедур (политик) регистрации событий безопасности	+	+	+
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления		+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей			

1	2	3	4	5
VI. Антивирусная защита (АВЗ)				
АВЗ.0	Разработка правил и процедур (политик) антивирусной защиты	+	+	+
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
VII. Обнаружение вторжений (СОВ)				
СОВ.0	Разработка правил и процедур (политик) обнаружения вторжений			+
СОВ.1	Обнаружение вторжений			+
СОВ.2	Обновление базы решающих правил			+
VIII. Контроль (анализ) защищенности информации (АНЗ)				
АНЗ.0	Разработка правил и процедур (политик) контроля (анализа) защищенности	+	+	+
АНЗ.1	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей	+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей		+	+
IX. Обеспечение целостности (ОЦЛ)				
ОЦЛ.0	Разработка правил и процедур (политик) обеспечения целостности	+	+	+
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных			
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+

1	2	3	4	5
ОЦЛ.4	Обнаружение и реагирование на поступление в автоматизированную систему управления незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к ее функционированию (защита от спама)			
ОЦЛ.5	Контроль содержания информации, передаваемой из автоматизированной системы управления (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации			
ОЦЛ.6	Ограничение прав пользователей по вводу информации в автоматизированную систему управления			+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в автоматизированную систему управления		+	+
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+
X. Обеспечение доступности (ОДТ)				
ОДТ.0	Разработка правил и процедур (политик) обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования системы		+	+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала	+	+	+
ОДТ.6	Кластеризация автоматизированной системы управления и (или) ее сегментов			
ОДТ.7	Контроль состояния и качества предоставления поставщиком телекоммуникационных услуг вычислительных ресурсов (мощностей), в том числе по передаче информации		+	+
XI. Защита среды виртуализации (ЗСВ)				
ЗСВ.0	Разработка правил и процедур (политик) защиты среды виртуализации	+	+	+

1	2	3	4	5
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей		+	+
XII. Защита технических средств (ЗТС)				
ЗТС.0	Разработка правил и процедур (политик) защиты технических средств	+	+	+
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования	+	+	+

1	2	3	4	5
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр			
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	+	+	+
XIII. Защита автоматизированной системы и ее компонентов (ЗИС)				
ЗИС.0	Разработка правил и процедур (политик) защиты автоматизированной системы и ее компонентов	+	+	+
ЗИС.1	Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления	+	+	+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств			
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными автоматизированными (информационными) системами			
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		+	+

1	2	3	4	5
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи			
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю			
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя			
ЗИС.14	Использование устройств терминального доступа для обработки информации			
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации		+	+
ЗИС.16	Выявление, анализ и блокирование скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			
ЗИС.17	Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов	+	+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.20	Защита беспроводных соединений, применяемых в автоматизированной системе управления	+	+	+

1	2	3	4	5
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы			
ЗИС.22	Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании	+	+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями	+	+	+
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения			
ЗИС.25	Использование в автоматизированной системе управления различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)			
ЗИС.26	Использование прикладного (специального) программного обеспечения, имеющего возможность функционирования в средах различных операционных систем			
ЗИС.27	Создание (эмуляция) ложных компонентов автоматизированной системы управления, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации			
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных технологиях и (или) структурно-функциональных характеристиках			
ЗИС.29	Перевод автоматизированной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев)			
ЗИС.30	Защита мобильных технических средств, применяемых в автоматизированной системе управления	+	+	+

1	2	3	4	5
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)				
ОБР.0	Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения	+	+	+
ОБР.1	Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения	+	+	+
ОБР.2	Статический анализ кода программного обеспечения в ходе разработки программного обеспечения		+	+
ОБР.3	Ручной анализ кода программного обеспечения в ходе разработки программного обеспечения			
ОБР.4	Тестирование на проникновение в ходе разработки программного обеспечения		+	+
ОБР.5	Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения		+	+
ОБР.6	Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)	+	+	+
XV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получение, проверку и установку обновлений)	+	+	+
ОПО.1	Получение обновлений программного обеспечения от разработчика или уполномоченного им лица	+	+	+
ОПО.2	Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне	+	+	+
ОПО.3	Централизованная установка обновлений программного обеспечения			
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)				
ПЛН.0	Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации	+	+	+
ПЛН.1	Определение лиц, ответственных за планирование, реализацию и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления	+	+	+
ПЛН.2	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированных системах управления	+	+	+
ПЛН.3	Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утвержденным планом	+	+	+
XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)				
ДНС.0	Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях	+	+	+

1	2	3	4	5
ДНС.1	Разработка плана действий на случай возникновения нештатных (непредвиденных) ситуаций	+	+	+
ДНС.2	Обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций	+	+	+
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций		+	+
ДНС.4	Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления на случай возникновения нештатных (непредвиденных) ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонент в случае возникновения нештатных (непредвиденных) ситуаций	+	+	+
XVIII. Информирование и обучение персонала (ИПО)				
ИПО.0	Разработка правил и процедур (политик) информирования и обучения персонала	+	+	+
ИПО.1	Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации	+	+	+
ИПО.2	Обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации	+	+	+
ИПО.3	Проведение практических занятий с персоналом по правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации		+	+
XIX.Анализ угроз безопасности информации и рисков от их реализации (УБИ)				
УБИ.0	Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации	+	+	+
УБИ.1	Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления	+	+	+
УБИ.2	Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)	+	+	+
XX. Выявление инцидентов и реагирование на них (ИНЦ)				
ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них	+	+	+
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	+	+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+	+	+

1	2	3	4	5
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов	+	+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	+	+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов	+	+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	+	+	+
XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)				
УКФ.0	Разработка правил и процедур (политик) управления конфигурацией автоматизированной системы управления и ее системы защиты	+	+	+
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и ее системы защиты	+	+	+
УКФ.2	Управление изменениями конфигурации автоматизированной системы управления и ее системы защиты	+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления	+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты	+	+	+
УКФ.5	Регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления	+	+	+

«+» - 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 уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в автоматизированной системе управления соответствующего класса защищенности.