Уральский Центр Систем Безопасности
Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

620100
г. Екатеринбург
ул. Ткачей, д. 6

тел.: +7(343) 379-98-34
факс: +7(343) 382-05-63

info@ussc.ru
www.USSC.ru

Аналитическая записка

Обзор приказа ФСТЭК России от 14.03.2014 №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Екатеринбург
2014

30 июня Минюстом был зарегистрирован новый нормативный документ, приказ ФСТЭК России от 14.03.2014 №31 (далее – Приказ), устанавливающий требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами 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 (далее – АСУ ТП).

Настоящий документ распространяется на вновь создаваемые (модернизируемые) АСУ ТП, вводимые в эксплуатацию после вступления в силу настоящего Приказа и не распространяется на АСУ ТП, обрабатывающие государственную тайну. Вместе с тем, ФСТЭК России рекомендует владельцам АСУ ТП спланировать (в случае технической возможности) поэтапное приведение своих систем управления в соответствие с настоящим документом.

Стоит отметить, что АСУ ТП рассматриваются как один из классов ключевых систем информационной инфраструктуры. Понятие же ключевой системы информационной инфраструктуры обобщает в себе множество различных классов информационных, автоматизированных систем и информационно-телекоммуникационных сетей (системы предупреждения и ликвидации чрезвычайных ситуаций, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и др. системы и сети).

Следующие методические документы ФСТЭК России могут применяться при защите АСУ ТП в качестве дополнительного методического материала, в части не противоречащей требованиям настоящего Приказа:

- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»;
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»;
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;
- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры».

По концепции и структуре требований Приказ во многом является схожим с 21-ым и 17-ым приказом ФСТЭК России и включает в себя блок требований к организации защиты информации в АСУ ТП, а также требования к мерам защиты информации.

Организация защиты информации

В рамках Приказа определяется многоуровневая структура АСУ ТП, приведенная на рисунке 1. Предложенная структура АСУ ТП включает три основных уровня, характеризующихся различным составом входящих в него компонентов.

Рисунок 1. Многоуровневая структура АСУ ТП

В качестве объектов защиты АСУ ТП выделяются:

- критически важная информация (технологическая информация), включающая управляющую, контрольно-измерительную информацию и др.;
- программно-технический комплекс, включающий технические средства, программное обеспечение (ПО) и средства защиты информации (СрЗИ).

В соответствии с Приказом защита информации, обрабатываемая в АСУ ТП, является составной частью работ по ее созданию и эксплуатации и обеспечивается на всех стадиях ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации в рамках системы защиты. При этом меры защиты информации должны:

- обеспечивать, в первую очередь, доступность и целостность информации и при необходимости ее конфиденциальность;
- соотноситься с мерами по промышленной, физической, пожарной, и т.п. мерами обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами.

Кроме того, отдельно подчеркивается, что используемые меры защиты не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированных систем управления производственными и технологическими процессами.

В Приказе выделяется 5 основных этапов обеспечения защиты информации в АСУ ТП, приведенных на рисунке 2.

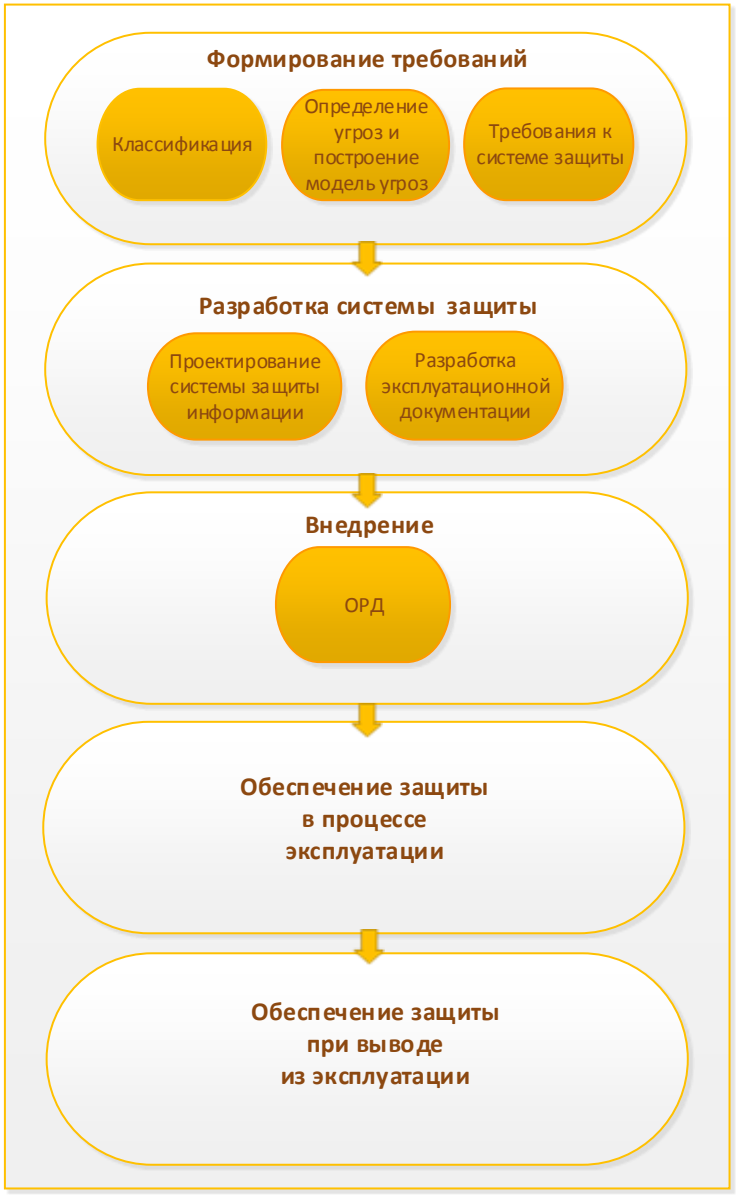

Рисунок 2. Этапы обеспечения защиты информации в АСУ ТП

На этапе формирования требований проводится *классификация АСУ ТП* и определение класса защищенности: К1 (самый высокий), К2 или К3.

Для определения класса защищенности необходимо определить уровень значимости обрабатываемой информации в зависимости от степени возможного ущерба от нарушения конфиденциальности, целостности или доступности обрабатываемой информации.

В случае обработки в АСУ ТП двух и более видов информации (измерительная информация, информация о состоянии процесса), уровень значимости определяется отдельно для каждого вида информации. Итоговый уровень значимости определяется по наивысшему значению из них или может быть установлен отдельно для каждого из уровней автоматизированных систем управления производственными и технологическими процессами и иных сегментов при их наличии.

Определение угроз безопасности информации и построение модели угроз производится на основании методических документов ФСТЭК России «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» и «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», включая:

- оценку возможностей нарушителей;
- анализ возможных сценариев реализации угроз безопасности информации;
- анализ последствий от нарушения свойств безопасности;
- и др.

Требования к системе защиты АСУ ТП определяются в зависимости от класса защищенности и актуальных угроз безопасности информации, включенных в модель угроз безопасности информации.

На этапе *разработки системы защиты* в рамках проектирования системы защиты информации осуществляется выбор СрЗИ, прошедших оценку соответствия, и определяются необходимые меры защиты с учетом особенностей функционирования ПО и технических средств на каждом уровне АСУ ТП. Стоит отметить, что форма оценки соответствия СрЗИ должна быть определена заказчиком в техническом задании в соответствии с Федеральным законом «О техническом регулировании».

Этап *внедрения системы защиты информации* включает следующие мероприятия:

- настройку ПО АСУ ТП;
- установку и настройку СрЗИ;
- проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний системы;
- анализ уязвимостей АСУ ТП, в рамках которого по решению заказчика может проводиться тестирование на проникновение;
- разработку документов, определяющих правила и процедуры, реализуемые для защиты информации.

Стоит отметить, что установка и настройка СрЗИ осуществляется в случаях, если такие средства необходимы для блокирования (нейтрализации) угроз безопасности информации, которые невозможно исключить настройкой АСУ ТП и должна обеспечивать корректность функционирования АСУ ТП, совместимость выбранных СрЗИ с ПО и техническими средствами АСУ ТП, а установленные СрЗИ не должны влиять на штатный режим функционирования системы.

Приказ не содержит положений, устанавливающих обязательную аттестацию АСУ ТП. Решение об аттестации АСУ ТП может быть принято заказчиком самостоятельно. В этом случае, аттестация системы защиты информации проводится в соответствии с национальными стандартами и методическим документами ФСТЭК России с оформлением соответствующих программ и методик аттестационных испытаний, протоколов и заключений.

Этапы обеспечения защиты информации *в ходе эксплуатации системы защиты* и при выводе ее из действия предусматривают реализацию определенных процедур управления информационной безопасностью, таких как:

- планирование мероприятий по обеспечению защиты в автоматизированных системах управления производственными и технологическими процессами;
- обеспечение действий в нештатных ситуациях;
- обучение персонала;
- выявление инцидентов в ходе эксплуатации и реагирование на них;
- контроль за обеспечением уровня защищенности;
- управление системой защиты, а также управление конфигурацией автоматизированных систем управления производственными и технологическими процессами;

- архивирование информации, а также уничтожение данных и остаточной информации при выводе автоматизированных систем управления производственными и технологическими процессами из эксплуатации.

Меры защиты информации

Помимо требований к организации защиты информации в АСУ ТП, Приказ определяет набор мер защиты информации, а также порядок их выбора, включающего:

- определение базового набора требований для установленного класса защищенности,
- адаптацию базового набора требований применительно к каждому уровню АСУ ТП, иным структурно-функциональным характеристикам и особенностям функционирования систем управления,
- уточнение адаптированного набора мер, в результате чего определяются меры защиты, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации на каждом из уровней АСУ ТП
- дополнение мерами, обеспечивающими выполнение требований к защите, установленных иными нормативными правовыми актами, национальными стандартами и другими руководящими документами
- возможность использования компенсирующих мер в случае, если отсутствует возможность реализации отдельных мер защиты на каком-либо из уровней АСУ ТП и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе из-за их негативного влияния на штатный режим функционирования АСУ ТП.

Состав мер защиты информации, описанных в документе, приведен в таблице 1. Каждая группы мер защиты включает требование по обязательному документированию соответствующей процедуры управления информационной безопасности. Кроме того, стоит отметить наличие требований по обеспечению безопасной разработки ПО и управлению конфигурацией АСУ ТП.

Таблица 1 – Наборы мер защиты информации

Условное обозначение	**Меры защиты информации**	**Кол-во требований**			
		К3	**К2**	**К1**	**Всего[1]**
ИАФ	Идентификация и аутентификация субъектов доступа и объектов доступа	6	7	7	8
УПД	Управление доступом субъектов доступа к объектам доступа	12	12	12	18
ОПС	Ограничения программной среды	2	3	4	5
ЗНИ	Защита машинных носителей информации	4	5	6	9

[1] Общее количество мер указано с учетом дополнительных мер, не включенных в базовые наборы защиты, сформированные в соответствии с классом автоматизированных систем управления производственными и технологическими процессами

Условное обозначение	Меры защиты информации	Кол-во требований			
		К3	К2	К1	Всего[1]
РСБ	Регистрация событий безопасности	7	8	8	9
АВЗ	Антивирусная защита	3	3	3	3
СОВ	Обнаружение вторжений	0	0	3	3
АНЗ	Контроль (анализ) защищенности информации	5	6	6	6
ОЦЛ	Обеспечение целостности	2	5	6	9
ОДТ	Обеспечение доступности	3	7	7	8
ЗСВ	Защита среды виртуализации	5	9	10	11
ЗТС	Защита технических средств	4	4	4	6
ЗИС	Защита автоматизированной системы и ее компонентов	8	11	11	31
ОБР	Обеспечение безопасной разработки программного обеспечения	3	6	6	7
ОПО	Управление обновлениями программного обеспечения	3	3	3	4
ПЛН	Планирование мероприятий по обеспечению защиты информации	4	4	4	4
ДНС	Обеспечение действий в нештатных ситуациях	4	6	6	6
ИПО	Информирование и обучение персонала	3	4	4	4
УБИ	Анализ угроз безопасности информации и рисков от их реализации	3	3	3	3
ИНЦ	Выявление инцидентов и реагирование на них	7	7	7	7
УКФ	Управление конфигурацией автоматизированной системы управления и ее системы защиты	6	6	6	6

В случае использования СрЗИ, прошедших оценку соответствии в форме обязательной сертификации, для реализации технических мер защиты информации, СрЗИ должны удовлетворять определенным требованиям, приведенным в таблице 4.

Таблица 4 - Выбор используемых СрЗИ в зависимости от класса защищенности АСУ

Класс СрЗИ	**Класс защищенности АСУ ТП**			
	3	**2**	**1**	
			отсутствие подключения к сети Интернет	**подключение к сети Интернет**
Средства вычислительной техники	≥ 5	≥ 5	≥ 5	
Системы обнаружения вторжений	≥ 5	≥ 4	≥ 4	
Антивирус	≥ 5	≥ 4	≥ 4	
Межсетевые экраны	≥ 4	≥ 4	≥ 4	≥ 3
Отсутствие недекларированных возможностей	≥ 4	≥ 4	—	
Средства доверенной загрузки	≥ 5	≥ 4	≥ 4	
Средства контроля съемных носителей информации	≥ 5	≥ 4	≥ 4	

Таким образом, данный Приказ определяет комплексный подход к обеспечению защиты информации, обрабатываемой в АСУ ТП, включающий организационные и технические меры по защите информации на всех стадиях жизненного цикла АСУ ТП.