Заместитель руководителя Управления
ФСТЭК России по Сибирскому федеральному округу

БУЛГАКОВ Виктор Николаевич

Требования к созданию систем безопасности значимых объектов критической инфраструктуры Российской Федерации и обеспечения их функционирования

Основания разработки Требований

Федеральный закон
от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Пункт 4 части 3 статьи 6:

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ФСТЭК России) устанавливает требования к созданию систем безопасности таких объектов и обеспечению их функционирования.

Часть 1 статьи 10:

В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

Структура НПА ФСТЭК России

ФСТЭК России
ПРИКАЗ
от 21 декабря 2017 г. № 235

Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

I. Общие положения

II.Требования к силам обеспечения безопасности значимых объектов КИИ

III. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ

IV. Требования к организационно-распорядительным документам по безопасности значимых объектов

V. Требования к функционированию систем безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ

Система безопасности значимых объектов

Система безопасности

Правовые меры

Организац. меры

Технические меры

Другие меры

Объекты КИИ субъекта

$ИС_1$ (знач.)	$АСУ\ ТП_1$	$ИТКС_1$ (знач.)
$ИС_2$	$АСУ\ ТП_2$ (знач.)	$ИТКС_2$
…	…	…
$Ис_n$ (знач.)	$АСУ\ ТП_l$	$ИТКС_m$ (знач.)

Создается в целях обеспечения устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак

Состав системы безопасности значимых объектов

- подразделения (работники) субъекта КИИ, ответственные за обеспечение безопасности значимых объектов КИИ;
- иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов КИИ, включая:
  - подразделения (работников), эксплуатирующие (эксплуатирующих) значимые объекты КИИ,
  - подразделения (работников), обеспечивающие (обеспечивающих) функционирование (сопровождение, обслуживание, ремонт) значимых объектов КИИ

программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов

разрабатываются субъектами критической информационной инфраструктуры в соответствии с Требованиями

Задачи системы безопасности значимых объектов

предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов

восстановление функционирования значимых объектов

ГОССОПКА

непрерывное **взаимодействие с ГосСОПКА**

Силы системы безопасности значимых объектов

определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов

руководитель субъекта КИИ

организация – лицензиат (ТЗИ или ТЗКИ)

создает систему безопасности, организует и контролирует ее функционирование, а также принимает меры по ее совершенствованию

уполномоченное лицо

должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов

подразделения, эксплуатир. значимые объекты

должны обеспечивать безопасность эксплуатируемых ими значимых объектов

подразделения, обеспечивающ. функционир. значимых объектов

осуществляют свои функции в соответствии с правилами безопасности, установленными организационно-распорядительными документами

подразделение, ответственное за обеспечение безопасности значимых объектов

выполняют только задачи, определенные в должностных регламентах и связанные с обеспечением безопасности значимых объектов или обеспечением информационной безопасности субъекта КИИ

Функции структурного подразделения по безопасности

- ✓ разработка предложений по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и представление их руководителю субъекта КИИ (уполномоченному лицу);
- ✓ проведение анализа угроз безопасности информации в отношении значимых объектов и выявление уязвимостей в них;
- ✓ обеспечение реализации требований по обеспечению безопасности значимых объектов;
- ✓ обеспечение в соответствии с требованиями по обеспечению безопасности значимых объектов реализации организационных мер и применения средств защиты информации, эксплуатации средств защиты информации;
- ✓ осуществление реагирования на компьютерные инциденты;
- ✓ организация проведения оценки соответствия значимых объектов требованиям по безопасности;
- ✓ подготовка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов;
- ✓ обладание знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов;
- ✓ прохождение повышения уровня знаний по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации не реже одного раза в год.

Средства системы безопасности значимых объектов

- Прошли оценку соответствия в форме обязательной сертификации, приемки или испытаний
- В приоритетном порядке применяются встроенные в ОПО и СПО СЗИ
- Применяются в соответствии с эксплуатационной документацией
- Должна быть обеспечена поддержка СЗИ
- Должны быть учтены возможные ограничения со стороны разработчика
- Должны обеспечивать реализацию технических мер обеспечения безопасности

-  встроенные в общесистемное, прикладное программное обеспечение средства защиты информации
- межсетевые экраны 
-  средства обнаружения (предотвращения) вторжений
- средства антивирусной защиты 
-  средства (системы) контроля (анализа) защищенности
- средства управления событиями безопасности 
-  средства защиты каналов передачи данных

Требования к организационно-распорядительным документам по безопасности значимых объектов

Организационно-распорядительные документы по безопасности значимых объектов должны определять:

- ✓ цели и задачи обеспечения безопасности значимых объектов
- ✓ основные угрозы безопасности информации и категории нарушителей
- ✓ основные организационные и технические мероприятия по обеспечению безопасности значимых объектов
- ✓ состав и структуру системы безопасности и функции ее участников
- ✓ порядок применения, формы оценки соответствия значимых объектов и СЗИ

- ✓ правила безопасной работы работников субъекта КИИ на значимых объектах
- ✓ действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций

- ✓ планы мероприятий по обеспечению безопасности значимых объектов
- ✓ порядок реализации отдельных мер по обеспечению безопасности значимых объектов
- ✓ порядок проведения испытаний или приемки средств защиты информации
- ✓ порядок реагирования на компьютерные инциденты
- ✓ порядок информирования и обучения работников субъекта КИИ
- ✓ порядок взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов
- ✓ порядок взаимодействия субъекта КИИ с ГосСОПКА

Являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта КИИ, доводятся в части касающейся

Состав и формы документов определяются субъектом КИИ

Требования к функционированию системы безопасности значимых объектов

планирование и разработка мероприятий по обеспечению безопасности значимых объектов

реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов

контроль состояния безопасности значимых объектов

совершенствование безопасности значимых объектов

Планирование и разработка мероприятий по обеспечению безопасности значимых объектов

Утверждаю
руководитель субъекта КИИ

План мероприятий по обеспечению безопасности значимых объектов

Мероприятие № 1

Наименование мероприятия.
Срок исполнения мероприятия.
Наименования подразделений (работников), ответственных за реализацию мероприятия.

…

Мероприятие № n

Наименование мероприятия.
Срок исполнения мероприятия.
Наименования подразделений (работников), ответственных за реализацию мероприятия.

Разрабатывается не менее чем на 1 год
Доводится до подразделений в части, их касающейся

Разрабатывается структурным подразделением по безопасности с участием подразделений, эксплуатирующих значимые объекты и подразделений, обеспечивающих их функционирование

Включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности значимых объектов, направленные на решение задач системы обеспечения безопасности

Контроль за выполнением плана мероприятий осуществляется структурным подразделением по безопасности

Подразделение по безопасности ежегодно готовит отчет о выполнении плана мероприятий, который представляется руководителю субъекта КИИ

Может быть включен в общий план деятельности субъекта КИИ в качестве отдельного раздела

Порядок разработки, утверждения и внесения изменений в план мероприятий определяется в организационно-распорядительных документах по безопасности значимых объектов

Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов

Выполнение плана мероприятий

В соответствии с организационно-распорядительными документами

Принятие мер

Организационных	Применение СЗИ

Документирование результатов

В соответствии с организационно-распорядительными документами

Контроль состояния безопасности значимых объектов

Проводится ежегодно

Внутренний контроль организации работ по обеспечению безопасности значимых объектов и эффективности принимаемых организационных и технических мер

Внешняя оценка (внешний аудит) состояния безопасности значимых объектов

Проводит **комиссия**, назначаемая субъектом КИИ, **в состав** которой **входят работники структурного подразделения по безопасности, работники подразделений, эксплуатирующих значимые объекты, и подразделений, обеспечивающих их функционирование**

Проводят **организации**, имеющие **лицензии на деятельность в области ЗИ** (в части услуг по контролю защищенности информации от НСД и ее модификации в средствах и системах информатизации)

Акт, подписываемый членами комиссии и утверждаемый руководителем субъекта (уполномоченным лицом)

Выявленные замечания подлежат устранению в порядке и сроки, установленные руководителем субъекта КИИ (уполномоченным лицом)

Совершенствование безопасности значимых объектов

Осуществляется структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты, и подразделений (работников), обеспечивающих функционирование значимых объектов

Проведение анализа

- функционирования системы безопасности
- состояния безопасности значимых объектов

Разработка предложений

- по развитию системы безопасности
- по мерам по совершенствованию безопасности значимых объектов

Предложения представляются руководителю субъекта КИИ

Предложения могут быть внесены в план мероприятий (по решению руководителя субъекта КИИ)

СПАСИБО ЗА ВНИМАНИЕ!