



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**

П Р И К А З

« » декабря 2017 г.

Москва

№ _____

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

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемые Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

2. Установить, что указанные в пункте 1 настоящего приказа Требования вступают в силу с 1 января 2018 г.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

В.СЕЛИН

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «___» декабря 2017 г. № ___

**Требования
к созданию систем безопасности
значимых объектов критической информационной инфраструктуры
Российской Федерации и обеспечению их функционирования**

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) и устанавливают требования к созданию субъектами критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) систем безопасности значимых объектов критической информационной инфраструктуры (далее – системы безопасности) и обеспечению их функционирования.

2. Реализация настоящих Требований является обязательной при обеспечении субъектами критической информационной инфраструктуры безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании.

3. Системы безопасности создаются субъектами критической информационной инфраструктуры в рамках комплекса правовых, организационных, технических и иных мер, направленных на обеспечение информационной безопасности (защиты информации) субъектов критической информационной инфраструктуры.

4. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак.

Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры для одного или группы значимых объектов критической информационной инфраструктуры могут создаваться отдельные системы безопасности.

5. Системы безопасности включают силы обеспечения безопасности значимых объектов критической информационной инфраструктуры и

используемые ими средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.

К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры, и иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов критической информационной инфраструктуры, включая подразделения (работников), эксплуатирующие (эксплуатирующих) значимые объекты критической информационной инфраструктуры, и подразделения (работников), обеспечивающие (обеспечивающих) функционирование (сопровождение, обслуживание, ремонт) значимых объектов критической информационной инфраструктуры.

К средствам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Системы безопасности должны функционировать в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов критической информационной инфраструктуры, разрабатываемыми субъектами критической информационной инфраструктуры в соответствии с настоящими Требованиями (далее – организационно-распорядительные документы по безопасности значимых объектов).

6. Основными задачами систем безопасности являются:

предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

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

восстановление функционирования значимых объектов критической информационной инфраструктуры, в том числе за счет создания и хранения резервных копий необходимой для этого информации;

непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляется в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации».

7. Создаваемые системы безопасности должны соответствовать требованиям:

к силам обеспечения безопасности значимых объектов критической информационной инфраструктуры;

к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

к организационно-распорядительным документам по безопасности значимых объектов;

к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

II. Требования к силам обеспечения безопасности значимых объектов критической информационной инфраструктуры

8. Руководство системой безопасности осуществляет руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее – уполномоченное лицо).

Руководитель субъекта критической информационной инфраструктуры (уполномоченное лицо) создает систему безопасности, организует и контролирует ее функционирование, а также принимает меры по ее совершенствованию.

9. Руководитель субъекта критической информационной инфраструктуры определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества, масштаба, сложности значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры.

10. Руководитель субъекта критической информационной инфраструктуры создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – штатные специалисты).

Структурное подразделение по безопасности, штатные специалисты выполняют следующие основные функции:

разрабатывают предложения по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и

представляют их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу);

проводят анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявляют уязвимости в них;

обеспечивают реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - требования по безопасности);

обеспечивают в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;

осуществляют реагирование на компьютерные инциденты в порядке, установленном в соответствии пунктом 6 части 4 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

организуют проведение оценки соответствия значимых объектов критической информационной инфраструктуры требованиям по безопасности;

готовят предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры.

Структурное подразделение по безопасности, штатные специалисты реализуют указанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры.

11. Для выполнения отдельных функций, предусмотренных пунктом 10 настоящих Требований, субъектами критической информационной инфраструктуры могут привлекаться организации, имеющие в зависимости от информации, обрабатываемой значимым объектом критической информационной инфраструктуры, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации (далее – лицензии в области защиты информации).

12. Работники структурного подразделения по безопасности, штатные специалисты должны обладать знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов критической информационной инфраструктуры в соответствии с настоящими Требованиями и требованиями по безопасности.

Работники структурного подразделения по безопасности, на которых непосредственно возложены обязанности обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также штатные

специалисты в соответствии со штатным расписанием субъекта критической информационной инфраструктуры должны иметь высшее или среднее профессиональное образование по направлениям подготовки (специальностям) «Информационная безопасность» или иное высшее или среднее профессиональное образование и при этом пройти обучение по программам профессиональной переподготовки по одной из специальностей по направлениям подготовки (специальностям) «Информационная безопасность».

Субъектом критической информационной инфраструктуры в соответствии с законодательством Российской Федерации организуется периодическое (не реже 1 раза в 5 лет) повышение квалификации работников структурного подразделения по безопасности, штатных специалистов.

13. Не допускается возложение на структурное подразделение по безопасности, штатных специалистов функций, не связанных с обеспечением безопасности значимых объектов критической информационной инфраструктуры или обеспечением информационной безопасности субъекта критической информационной инфраструктуры в целом.

Обязанности, возлагаемые на работников структурного подразделения по безопасности, штатных специалистов, должны быть определены в их должностных регламентах (должностных инструкциях).

14. Подразделения, эксплуатирующие значимые объекты критической информационной инфраструктуры, обеспечивают безопасность эксплуатируемых ими значимых объектов критической информационной инфраструктуры. Объем возлагаемых на подразделения задач определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

По решению субъекта критической информационной инфраструктуры в подразделениях, эксплуатирующих значимые объекты критической информационной инфраструктуры, могут также назначаться работники, на которых возлагаются отдельные функции по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Возложенные на работников функции включаются в их должностные регламенты (должностные инструкции).

Координацию и контроль деятельности указанных работников по вопросам обеспечения безопасности значимых объектов критической информационной инфраструктуры осуществляют структурное подразделение по безопасности, штатные специалисты.

15. Работники, эксплуатирующие значимые объекты критической информационной инфраструктуры (пользователи), а также работники, обеспечивающие функционирование значимых объектов критической информационной инфраструктуры, выполняют свои обязанности на значимых объектах критической информационной инфраструктуры в соответствии с правилами безопасности, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами).

До работников должны быть доведены положения организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся.

Субъект критической информационной инфраструктуры не реже 1 раза в год организует проведение методических занятий, лекций, семинаров, иных мероприятий, направленных на повышение осведомленности об угрозах безопасности информации и уровня знаний указанных работников по вопросам обеспечения безопасности критической информационной инфраструктуры.

16. Организации, привлекаемые на основании договора субъектом критической информационной инфраструктуры для эксплуатации, обеспечения функционирования значимых объектов критической информационной инфраструктуры и (или) для обеспечения их безопасности, должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов в части, их касающейся.

В договорах должна быть предусмотрена обязанность привлекаемых организаций обеспечивать соблюдение требований субъекта критической информационной инфраструктуры, установленных организационно-распорядительными документами по безопасности значимых объектов, в той части, в которой они были ознакомлены.

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

17. К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры, относятся средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства обнаружения (предотвращения) вторжений (компьютерных атак), средства антивирусной защиты, средства (системы) контроля (анализа) защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

18. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку соответствия требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или

с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

19. Параметры и характеристики применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры, принимаемыми в соответствии с требованиями по безопасности.

В качестве средств защиты информации в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов критической информационной инфраструктуры (при их наличии).

20. Средства защиты информации должны применяться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации.

21. Применяемые средства защиты информации должны быть обеспечены гарантийной, технической поддержкой.

При выборе средств защиты информации необходимо учитывать наличие ограничений на возможность их применения субъектом критической информационной инфраструктуры на любом из принадлежащих ему значимых объектов критической информационной инфраструктуры со стороны разработчиков (производителей) или иных лиц.

22. Порядок применения средств защиты информации определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта критической информационной инфраструктуры.

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

23. Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности утверждаются организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Организационно-распорядительные документы по безопасности значимых объектов разрабатываются в рамках общей системы документов (стандартов организации) по вопросам обеспечения информационной безопасности (защиты информации) субъекта критической информационной инфраструктуры. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры, могут быть

включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта критической информационной инфраструктуры.

24. Организационно-распорядительные документы по безопасности значимых объектов разрабатываются применительно к особенностям деятельности субъекта критической информационной инфраструктуры на основе настоящих Требований, требований по безопасности, иных нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры и защиты информации, а также с учетом международных, национальных стандартов и стандартов организаций в данной области.

25. Организационно-распорядительные документы по безопасности значимых объектов должны определять:

а) цели и задачи обеспечения безопасности значимых объектов критической информационной инфраструктуры, основные угрозы безопасности информации и категории нарушителей, основные организационные и технические мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, проводимые субъектом критической информационной инфраструктуры, состав и структуру системы безопасности и функции ее участников, порядок применения, формы оценки соответствия значимых объектов критической информационной инфраструктуры и средств защиты информации требованиям по безопасности;

б) планы мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, модели угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры, порядок реализации отдельных мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры, порядок проведения испытаний или приемки средств защиты информации, порядок реагирования на компьютерные инциденты, порядок информирования и обучения работников, порядок взаимодействия подразделений (работников) субъекта критической информационной инфраструктуры при решении задач обеспечения безопасности значимых объектов критической информационной инфраструктуры, порядок взаимодействия субъекта критической информационной инфраструктуры с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

в) правила безопасной работы работников субъекта критической информационной инфраструктуры на значимых объектах критической информационной инфраструктуры, действия работников субъекта критической информационной инфраструктуры при возникновении компьютерных инцидентов и иных нештатных ситуаций.

Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются субъектом критической информационной инфраструктуры с учетом особенностей его деятельности.

26. Организационно-распорядительные документы по безопасности значимых объектов утверждаются руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом). По решению руководителя субъекта критической информационной инфраструктуры отдельные организационно-распорядительные документы по безопасности значимых объектов могут утверждаться иными уполномоченными на это лицами субъекта критической информационной инфраструктуры.

27. Организационно-распорядительные документы по безопасности значимых объектов должны быть доведены до руководства субъекта критической информационной инфраструктуры, подразделения по безопасности, штатных специалистов, а также до иных подразделений (работников), участвующих в обеспечении безопасности значимых объектов критической информационной инфраструктуры, в части, их касающейся.

V. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры

28. В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрены следующие процессы:

планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

контроль состояния безопасности значимых объектов критической информационной инфраструктуры;

совершенствование безопасности значимых объектов критической информационной инфраструктуры.

29. В рамках планирования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее – план мероприятий).

По решению субъекта критической информационной инфраструктуры план мероприятий может разрабатываться на более длительный срок с учетом имеющихся программ (планов) по модернизации (дооснащению) значимых объектов критической информационной инфраструктуры.

План мероприятий разрабатывается структурным подразделением по безопасности, штатными специалистами с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной

инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.

План мероприятий должен содержать наименования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, сроки их выполнения, наименования подразделений (работников), ответственных за реализацию каждого мероприятия.

В план мероприятий включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, направленные на решение задач, установленных пунктом 6 настоящих Требований.

Разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляется в соответствии с настоящими Требованиями, требованиями по безопасности, иными нормативными правовыми актами по обеспечению безопасности критической информационной инфраструктуры, а также организационно-распорядительными документами по безопасности значимых объектов.

План мероприятий утверждается руководителем субъекта критической информационной инфраструктуры и доводится до подразделений (работников) субъекта критической информационной инфраструктуры в части, их касающейся.

В подразделениях, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделениях, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры, на основе утвержденного плана мероприятий могут разрабатываться соответствующие отдельные планы мероприятий.

Контроль за выполнением плана мероприятий осуществляется структурным подразделением по безопасности, штатными специалистами. Структурное подразделение по безопасности, штатные специалисты ежегодно готовят отчет о выполнении плана мероприятий, который представляется руководителю субъекта критической информационной инфраструктуры.

Мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут включаться в общий план деятельности субъекта критической информационной инфраструктуры (в случае его разработки) отдельным разделом.

Порядок разработки, утверждения и внесения изменений в план мероприятий определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

30. Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры является результатом выполнения плана мероприятий и осуществляется в соответствии с

организационно-распорядительными документами по безопасности значимых объектов.

В ходе реализации мероприятий по обеспечению безопасности значимых объектов принимаются организационные меры и (или) внедряются средства защиты информации на значимых объектах критической информации, направленные на блокирование (нейтрализацию) угроз безопасности информации.

Результаты реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры подлежат документированию в порядке, установленном субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

31. В рамках контроля состояния безопасности значимых объектов критической информационной инфраструктуры осуществляется внутренний контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер.

Контроль проводится на соответствие настоящим Требованиям, требованиям по безопасности, иным нормативным правовым актам в области обеспечения безопасности критической информационной инфраструктуры, а также организационно-распорядительным документам по безопасности значимых объектов.

Контроль проводится ежегодно комиссией, назначаемой субъектом критической информационной инфраструктуры. В состав комиссии включаются работники структурного подразделения по безопасности, штатные специалисты, подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры в состав комиссии могут включаться работники иных подразделений субъекта критической информационной инфраструктуры.

Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут применяться средства контроля (анализа) защищенности.

Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом).

В случае проведения по решению руководителя субъекта критической информационной инфраструктуры внешней оценки (внешнего аудита) состояния безопасности значимых объектов критической информационной инфраструктуры внутренний контроль может не проводиться.

Для проведения внешней оценки привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по

контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации).

32. В рамках совершенствования безопасности значимых объектов критической информационной инфраструктуры проводится анализ функционирования системы безопасности и состояния безопасности значимых объектов критической информационной инфраструктуры, по результатам которых разрабатываются предложения по развитию системы безопасности и меры по совершенствованию безопасности значимых объектов критической информационной инфраструктуры.

Анализ функционирования системы безопасности, а также разработка предложений по совершенствованию безопасности значимых объектов критической информационной инфраструктуры осуществляются структурным подразделением по безопасности, штатными специалистами с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.

Предложения по совершенствованию безопасности значимых объектов критической информационной инфраструктуры представляются руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу).

В соответствии с решением руководителя субъекта критической информационной инфраструктуры (уполномоченного лица) предложения по совершенствованию безопасности значимых объектов критической информационной инфраструктуры включаются в план мероприятий, разрабатываемый в соответствии с пунктом 29 настоящих Требований.
