ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« » декабря 2017 г. Москва № _____

Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

В соответствии с пунктом 3 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**:

Утвердить прилагаемую форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

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

Форма
направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Ограничительная пометка
или гриф секретности
(при необходимости)

1. Сведения об объекте критической информационной инфраструктуры

Наименование объекта	
Адреса размещения объекта[1]	
Сфера (область) деятельности, в которой функционирует объект[2]	
Назначение объекта	
Критические процессы, которые обеспечиваются объектом[3]	
Архитектура объекта[4]	

2. Сведения о субъекте критической информационной инфраструктуры

Наименование субъекта	
Адрес (местонахождение) субъекта	
Адрес фактического местонахождения субъекта	
Руководитель субъекта[5]	
Лицо, на которое возложены функции обеспечения безопасности объектов[6]	

Структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов[7]	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

Категория сети электросвязи[8]	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи[9]	
Способ взаимодействия с сетью электросвязи [10]	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

Наименование лица, эксплуатирующего объект	
Адрес (местонахождение) лица, эксплуатирующего объект	
Адрес фактического местонахождения лица, эксплуатирующего объект	
Элемент (компонент) объекта, который эксплуатируется лицом[11]	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

Программно-аппаратные средства[12]	
Общесистемное программное обеспечение[13]	

Прикладное программное обеспечение[14]	
Средства защиты информации[15]	

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

Категория нарушителя[16]	
Угрозы безопасности информации[17]	

7. Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов[18]	
Возможные последствия от компьютерных инцидентов[19]	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

Категория значимости объекта[20]	
Результаты оценки показателей[21]	

9. Организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры

Организационные меры[22]	
Технические меры[23]	

Примечания: 1. В случае, если объект критической информационной инфраструктуры является распределенным, указываются адреса подразделений (обособленных подразделений, филиалов,

представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты объекта критической информационной инфраструктуры (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства).

2. Указывается в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

3. Указываются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции, для обеспечения (управления, контроля) которых используется объект критической информационной инфраструктуры.

4. Указывается архитектура объекта: одноранговая сеть, клиент-серверная система, «тонкий клиент», сеть передачи данных, SCADA-система, распределенная система управления или иная архитектура.

5. Указываются наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта критической информационной инфраструктуры.

6. Указываются наименование должности, фамилия, имя, отчество (при наличии) должностного лица, на которое возложено обеспечение безопасности значимых объектов. В случае отсутствия у субъекта такого должностного лица указываются наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта критической информационной инфраструктуры. В случае неприсвоения объекту ни одной из категорий значимости сведения не указываются.

7. Указываются наименование подразделения, ответственного за обеспечение безопасности значимых объектов, наименование должности, фамилия, имя, отчество (при наличии) руководителя подразделения, рабочий телефон, адрес электронной почты (при наличии). В случае назначения штатных специалистов указываются сведения по каждому специалисту. В случае неприсвоения объекту ни одной из категорий значимости сведения не указываются.

8. Указывается категория сети электросвязи: сеть связи общего пользования, выделенная сеть связи, технологическая сеть связи, присоединенная к сети связи общего пользования, сеть связи специального назначения или другая сеть связи для передачи информации при помощи электромагнитных систем. В случае, если объект критической информационной инфраструктуры не взаимодействует с сетями электросвязи, указываются сведения

об отсутствии такого взаимодействия.

9. Указывается цель взаимодействия с сетью электросвязи: передача (прием) информации, оказание услуг, управление, контроль технологическим, производственным оборудованием (исполнительным устройствами) или иные цели. В случае, если объект критической информационной инфраструктуры не взаимодействует с сетями электросвязи, сведения не указываются.

10. Указываются типы доступа к сети электросвязи (проводной, беспроводный), используемые технологии доступа, протоколы взимодействия. В случае, если объект критической информационной инфраструктуры не взаимодействует с сетями электросвязи, сведения не указываются.

11. Указывается в случае, если лицо эксплуатирует не весь объект, а один или несколько его отдельных элементов (компонентов): дата-центр, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства) или иные элементы (компоненты).

12. Указываются наименования программно-аппаратных средств и их количество: пользовательские компьютеры, серверы, телекоммуникационное оборудование, средства беспроводного доступа, технологическое, производственное оборудование (исполнительные устройства) или иные программно-аппаратные средства.

13. Указываются наименования клиентских, серверных операционных систем, средств виртуализации (при наличии).

14. Указываются наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются).

15. Указываются наименования средств защиты информации и реквизиты сертификатов соответствия на них. В случае отсутствия сертификатов соответствия указываются реквизиты иного документа, содержащего результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки. Для средств защиты информации, встроенных в программное обеспечение, указываются функции безопасности этого программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация или иные функции). В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации.

16. Указываются внешний или внутренний нарушитель, дается краткая характеристика основных возможностей нарушителей по реализации угроз безопасности информации в части их

оснащенности, знаний, мотивации. В случае неактуальности нарушителей для объекта критической информационной инфраструктуры приводится краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации.

17. Указываются основные угрозы безопасности информации. В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности.

18. Указываются типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак, или приводится обоснование невозможности наступления таких компьютерных инцидентов. В качестве типов компьютерных инцидентов рассматриваются: отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта.

19. Указывается ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», или приводится обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов.

20. Не указывается в случае неприсвоения объекту ни одной из категорий значимости.

21. Указываются полученные значения по каждому из показателей критериев значимости и обоснование полученных результатов. Также приводятся значения показателей в случае, если получены значения ниже нижних показателей, утверждаемых в соответствии с пунктом 1 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». В случае, если показатель не применим к объекту, делается отметка о его неприменимости с соответствующим обоснованием.

22. Указываются организационные меры: установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта. Меры указываются для действующих (эксплуатируемых) значимых объектов критической информационной инфраструктуры. В случае неприсвоения объекту ни одной из категорий значимости

сведения не указываются.

23. Указываются группы технических мер: идентификация и аутентификация, управление доступом, ограничение программной среды, антивирусная защита и иные группы мер в соответствии с требованиями по обеспечению безопасности значимых объектов. Меры указываются для действующих (эксплуатируемых) значимых объектов критической информационной инфраструктуры. В случае неприсвоения объекту ни одной из категорий значимости сведения не указываются.