ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«22» декабря 2017 г. Москва № 236

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 «22» декабря 2017 г. № 236

Форма

Сведения 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)

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	
1.4.	Назначение объекта	
1.5.	Критические процессы (управленческие, технологические,	

	производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электрон-	

	ной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	

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

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2.	Наименование оператора связи	
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	

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

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	

5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	

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

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	

6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	
7.2.	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 обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1.	Категория значимости, которая присвоена объекту	
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	

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

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	

_____	_____	_____
(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)	(подпись)	(инициалы, фамилия)
	М.П. (при наличии печати)	

«__» _____ 20___ г.