Утверждена
Приказом ФСТЭК России
от 22 декабря 2017 г. № 236
(в ред. Приказа ФСТЭК России
от 21.03.2019 № 59)

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

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры		
1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
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.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
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 электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	
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 и (или) провайдера хостинга	
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), протоколов взаимодействия	
4. Сведения о лице, эксплуатирующем объект критической нформационной 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)	
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	
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, 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 (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) 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	
8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры		
8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	

8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	
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 (подпись) (инициалы, фамилия) субъекта критической информационной инфраструктуры или уполномоченного им лица		
"__" _____ 2020 г.		
Рупор бумажной безопасности https://valerykomarov.blogspot.com		