Приложение 7

к Методическим рекомендациям

Форма сведений об объекте информационных систем и ресурсов

**Сведения об объекте ИСиР**

| **№** | **Параметр** | **Информация (пояснения по заполнению)** |
| --- | --- | --- |
| **Сведения об ИСиР** | | |
| 1 | Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети) |  |
| 2 | Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта |  |
| 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» |  |
| 4 | Назначение объекта |  |
| 5 | Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть) |  |
| 6 | Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура) |  |
| 7 | Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество |  |
| 9 | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем) |  |
| 10 | 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 |  |
| 11 | Наименование оператора связи и (или) провайдера хостинга |  |
| **Сведения об угрозах безопасности информации ИСиР** | | |
| 14 | 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 ИСиР |  |
| 15 | Основные угрозы безопасности информации или обоснование их неактуальности ИСиР |  |
| 16 | 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 |  |
| **Сведения об реализованных мерах по обеспечению безопасности ИСиР** | | |
| 17 | Реализованные организационные меры защиты |  |
| 18 | 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. |  |
| **Сведения о рекомендуемой к присвоению ИСиР категории значимости** | | |
| 19 | Категория значимости рекомендуемая |  |
| **Сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ (ФСТЭК России)** | | |
| 21 | Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта) и Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов |  |