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) | Указывается наименование ИСиР. Может использоваться произвольное наименование, основные критерии:  - оно должно быть уникальным в рамках Организации и однозначно идентифицировать систему;  - данное название должно использоваться во всех документах, касающихся данной системы |
| 2 | Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта | В случае, если ИСиР является распределённым, указываются адреса подразделений (обособленных подразделений, филиалов, представительств) ОИВ/организации, в которых размещаются сегменты объекта КИИ (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства).  Достаточная точность указания — уровень здания. В случае, если объект КИИ — ИТС, указывается место расположения сетевого оборудования (активного и пассивного) |
| 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» | Указывается в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности КИИ Российской Федерации»:  сфера здравоохранения, науки, транспорта, связи, энергетики, банковская сфера или сфера финансового рынка, топливно-энергетический комплекс, область атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности В случае, если объект функционирует в нескольких сферах – указываются все соответствующие сферы |
| 4 | Назначение объекта | Указывается задача / цель функционирования объекта, например: управление работой гидроагрегата, ведение единого учета граждан, записывающихся на прием к врачу в медицинских учреждениях г. Москвы, управление и контроль работы нефтеперерабатывающей установки; единый центр управления технологическими процессами обогатительного завода и т. д. |
| 5 | Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть) | Указываются тип ИСиР, должен совпадать с типом, указанным в п.1 при наименовании объекта |
| 6 | Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура) | Выбирается тип архитектуры из указанных вариантов или приводится уточнение их вариаций: одноранговая сеть, клиент-серверная система, «тонкий клиент», сеть передачи данных, SCADA-система, распределенная система управления или иная архитектура |
| 7 | Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество | Указываются наименования программно-аппаратных средств и их количество:   * пользовательские компьютеры, * серверы, * телекоммуникационное оборудование, * средства беспроводного доступа, * технологическое, производственное оборудование (исполнительные устройства) * иные программно-аппаратные средства |
| 9 | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем) | Указываются наименования прикладных программ |
| 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 | 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 ИСиР не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. ЛВС Организации также должна указываться, если она не входит в состав объекта КИИ и с ней осуществляется какое-либо взаимодействие |
| 11 | Наименование оператора связи и (или) провайдера хостинга | Указывается наименование соответственного юридического лица (нескольких лиц, если сетей электросвязи несколько).  В случае, если ИСиР не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия |
| **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 | Указываются сведения о потенциальных нарушителях. В случае отсутствия потенциальных нарушителей приводится обоснование (например: физически изолированная система, доступ только у доверенных лиц-администраторов, съемные носители не используются) |
| 15 | Основные угрозы безопасности информации или обоснование их неактуальности ИСиР | Указываются основные угрозы безопасности информации.  В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности. Актуально при отсутствии потенциальных нарушителей |
| 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 | Указывается общий перечень типов компьютерных инцидентов.  В случае отсутствия, приводится обоснование их неактуальности (возможно при отсутствии потенциальных нарушителей) |
| **Сведения об реализованных мерах по обеспечению безопасности ИСиР** | | |
| 17 | Реализованные организационные меры защиты | Указываются реализованные организационные меры защиты.  Для упрощения последующих работ лучше сразу указывать в виде мер из Приложения к [Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239](https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239) |
| 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. | Указываются сведения о соответствующих средствах защиты информации, используемых для обеспечения ИБ рассматриваемой ИСиР (наименования средств защиты информации, реквизиты сертификатов соответствия, если есть). Дополнительно рекомендуется указывать средства защиты, используемые на периметре ЛВС ОИВ/организации, которые используются для защиты инфраструктуры в целом от внешних нарушителей – с соответствующим уточнением, что для защиты от внешних нарушителей.  Для средств защиты информации, встроенных в программное обеспечение, указываются функции безопасности этого программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, иные функции).  Для упрощения последующих работ лучше сразу уточнять какую из мер Приложения к [Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017г. № 239](https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239) реализуют указываемые средства защиты, *например*:   * *АВЗ.1, АВЗ.2 — средство антивирусной защиты \*\*\*\* Endpoint Security 10, сертификат ИТ.САВЗ.Б2.ПЗ № \*\*\*5;* * *СОВ.1, СОВ.2 — \*\*\*\* Security Gateway версии R77.10, сертификат ИТ.СОВ.С4.ПЗ № \*\*\*\*4;* * *ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД \*\*\*\*\*.*   В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации |
| **Сведения о рекомендуемой к присвоению ИСиР категории значимости** | | |
| 19 | Категория значимости рекомендуемая | Указываются категория значимости либо информация о неприсвоении объекту ни одной из таких категорий |
| **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 | Указывается соответствующий перечень необходимых мер, соответствующих рекомендуемой категории значимости, из Приложения к [Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239.](https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239)  *Пример:*  *‒ ИАФ.0 Разработка политики идентификации и аутентификации;*  *‒ ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов;*  *‒ ИАФ.2 Идентификация и аутентификация устройств; ‒ и т. д.*  В случае, если объекту КИИ не присвоена категория значимости, делается соответствующее указание  «Объект КИИ не является значимым – обязательных мер не установлено» |