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

Наименование объекта критической информационной инфраструктуры.

1. Сведения об объекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование объекта | Указывается наименование ИС / АСУ ТП / ИТС. 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 |
| Адреса размещения объекта | В случае, если объект КИИ является распределённым, указываются адреса подразделений (обособленных подразделений, филиалов, представительств) субъекта КИИ, 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) |
| Сфера (область) деятельности, в которой функционирует объект | 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 |
| 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. |
| Тип объекта | (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть) |
| Архитектура объекта | 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 |

1. Сведения о субъекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование субъекта | Наименование субъекта КИИ — лица, которое владеет объектом КИИ |
| Адрес местонахождения субъекта | Юридический адрес  Адрес фактического местонахождения субъекта (если отличается) |
| Должность, фамилия, имя, отчество (при наличии) руководителя субъекта | Должность, Ф.И.О. руководителя |
| Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов | Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов.  В случае отсутствия такого должностного лица — наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта |
| 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) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии) | Указываются соответствующие данные:  ‒ Структурное подразделение, ответственное за обеспечение безопасности значимых объектов;  ‒ Должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии). Или, в случае отсутствия выделенного подразделения  ‒ должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии) |
| ИНН субъекта и КПП его обособленных подразделений | Указываются соответствующие данные:  ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта |

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

|  |  |
| --- | --- |
| Категория сети электросвязи или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи | Указывается категория сети электросвязи (в соответствии с 126-ФЗ): 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 КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия.  ЛВС (КСПД) Организации также должна указываться, если она не входит в состав объекта КИИ и с ней осуществляется какое-либо взаимодействие. |
| Наименования оператора связи | Наименование оператора связи и (или) провайдера хостинга Указывается наименование соответственного юридического лица (нескольких лиц, если сетей электросвязи несколько). В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. |
| Цель взаимодействия с сетью электросвязи | Указывается цель взаимодействия с сетью электросвязи: передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель.  В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. |
| Способ взаимодействия с сетью электросвязи | Указывается соответствующая информация о взаимодействии с сетями электросвязи: тип доступа к сети электросвязи (проводной, беспроводный), используемых технологий доступа, протоколов взаимодействия.  В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. |

1. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование лица, эксплуатирующего объект | Наименование субъекта КИИ — лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта)  В случае, если эксплуатацию осуществляет субъект КИИ — указываются его данные |
| Адрес местонахождения лица, эксплуатирующего объект | Юридический адрес лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта).  Адрес фактического местонахождения субъекта (если отличается) лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта).  В случае, если эксплуатацию осуществляет субъект КИИ — указываются его данные |
| Элемент (компонент) объекта, который эксплуатируется лицом | Указываются соответствующие компоненты / сегменты/ зоны ответственности в случае, если эксплуатацией объекта занимается лицо, отличающееся от субъекта КИИ.  В случае, если эксплуатацию осуществляет субъект КИИ — указывается «объект целиком эксплуатируется субъектом» |
| ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта | Указываются соответствующие данные:  ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений(филиалов, представительств), в которых размещаются сегменты распределенного объекта |

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

|  |  |
| --- | --- |
| Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество | Указываются наименования программно-аппаратных средств и их количество:  ‒ пользовательские компьютеры — х шт.,  ‒ серверы — х шт.,  ‒ телекоммуникационное оборудование — х шт.,  ‒ средства беспроводного доступа — х шт.,  ‒ технологическое, производственное оборудование (исполнительные устройства) — х шт.,  ‒ иные программно-аппаратные средства. |
| Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии) | Указываются наименования клиентских, серверных операционных систем, средств виртуализации (при наличии) |
| Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ,  входящих в состав дистрибутивов операционных систем) | Указываются наименования прикладных программ: наименование ERP, SCADA и иных прикладных продуктов, обеспечивающих выполнение функций объекта по его назначению |
| 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 рассматриваемого объекта КИИ (наименования средств защиты информации, реквизиты сертификатов соответствия, если есть).  Дополнительно рекомендуется указывать средства защиты, используемые на периметре КСПД (ЛВС) 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 2017 г. N 239 реализуют указываемые средства защиты, например:  ‒ АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат ИТ.САВЗ.Б2.ПЗ № 3025;  ‒ СОВ.1, СОВ.2 — Check Point Security Gateway версии R77.10, сертификат ИТ.СОВ.С4.ПЗ № 3634;  ‒ ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД HP C8R15A.  В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации |

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

|  |  |
| --- | --- |
| Категория нарушителя, 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 | Указываются сведения о потенциальных нарушителях, например:  Внешний нарушитель, обладающий средним потенциалом и высокой мотивацией, высокой квалификацией в области обнаружения и эксплуатации уязвимостей ИС.  Данный тип нарушителя обладает следующими возможностями:  ‒ возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами КЗ;  ‒ возможность сбора дополнительной информации о структурно-функциональных характеристиках и мерах защиты информации, применяемых в ИС;  ‒ возможность получить информацию об уязвимостях компонентов ИС, а также методах и средствах реализации угроз:   * опубликованную в общедоступных источниках; * путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО.   Данный тип нарушителя может использовать следующие каналы реализации угроз:  ‒ информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет);  ‒ беспроводные каналы передачи данных;  ‒ каналы связи, выходящие за пределы контролируемой зоны;  ‒ отчуждаемые носители информации и мобильные устройства, выносимые за пределы контролируемой зоны;  ‒ направленные воздействий на работников Организации (социальная инженерия).  Внутренний нарушитель, обладающий низким потенциалом, низкой мотивацией и квалификацией продвинутого пользователя с ограниченными знаниями в области обнаружения и эксплуатации уязвимостей ИС.  Данный тип нарушителя обладает следующими возможностями:  ‒ самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами КЗ;  ‒ сбора дополнительной информации о структурно-функциональных характеристиках и мерах защиты информации, применяемых в ИС;  ‒ получать информацию о пользователях и характеристиках ИС;  ‒ осуществлять попытки физического или логического доступа к ИС в рамках реализованных мер защиты  ‒ получать информацию об уязвимостях компонентов ИС, а также методах и средствах реализации угроз:   * опубликованную в общедоступных источниках; * путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО.   Данный тип нарушителя может использовать следующие каналы реализации угроз:  ‒ информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет);  ‒ беспроводные каналы передачи данных;  ‒ каналы связи, по которым осуществляется передача информации ограниченного доступа;  ‒ каналы связи, по которым осуществляется передача информации ограниченного доступа;  ‒ отчуждаемые носители информации и мобильные устройства;  ‒ направленные воздействий на работников Организации (социальная инженерия) |
| Основные угрозы безопасности информации или обоснование их неактуальности | Указываются основные угрозы безопасности информации. В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности (допускается в случае отсутствия потенциальных нарушителей и каналов реализации угроз) |

1. Возможные последствия в случае возникновения компьютерных инцидентов

|  |  |
| --- | --- |
| Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак | Указываются типы инцидентов из предложенных или дополняются/уточняются собственными: отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта.  В случае отсутствия актуальных угроз безопасности информации указывается невозможность наступления компьютерных инцидентов |

1. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

|  |  |
| --- | --- |
| Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий | Устанавливаются 3 категории значимости. Самая высокая категория - первая, самая низкая - третья. Если нет категории то пишется без категории |
| Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту | Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения берутся из 127- ПП  - Социальная значимость Причинение ущерба жизни и здоровью людей (человек)  - Политическая значимость  - Экономическая значимость  - Экологическая значимость  - Значимость для обеспечения обороны страны, безопасности государства и правопорядка |
| Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту | Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту я из 127- ПП |

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

|  |  |
| --- | --- |
| Организационные меры по обеспечению безопасности объекта | Указывается соответствующий перечень необходимых организационных мер, соответствующих присвоенной объекту КИИ категории значимости, из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239  В случае, если объекту КИИ не присвоена категория значимости, делается соответствующее указание «Объект КИИ не является значимым — обязательных мер не установлено» |
| Технические меры по обеспечению безопасности объекта | Указывается соответствующий перечень технических мер, соответствующих присвоенной объекту КИИ категории значимости, из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239, например:  ‒ 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» |