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) | Аппарат ИВЛ МК-1 |
| 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» | Здравоохранение |
| 1.4. | Назначение объекта | Проведение ингаляционной анестезии с искусственной вентиляцией легких |
| 1.5. | Тип объекта (информационная система, автоматизированная система управления или информационно-телекоммуникационная сеть) | Автоматизированная система управления |
| 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) | Система диспетчерского управления и контроля |

1. 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 |  |

1. 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 | Взаимодействие объекта критической информационной инфраструктуры и сетей электросвязи отсутствует |
| 3.2. | Наименование оператора связи и (или) провайдера хостинга | Взаимодействие объекта критической информационной инфраструктуры и сетей электросвязи отсутствует |
| 3.3. | Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Взаимодействие объекта критической информационной инфраструктуры и сетей электросвязи отсутствует |
| 3.4. | Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия | Взаимодействие объекта критической информационной инфраструктуры и сетей электросвязи отсутствует |

1. 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) |  |
| 4.4. | 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

|  |  |  |
| --- | --- | --- |
| 5.1. | Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество | Аппарат ИВЛ МК-1 – 1 |
| 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) | - МК-1 |
| 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 | Средства защиты информации отсутствуют |

1. 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 | 1. Преступные группы (криминальные структуры) (категория – внешний, уровень возможностей – Н2. Нарушитель, обладающий базовыми повышенными возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - же­лание са­море­али­зации (под­твержде­ние ста­туса).   1. Отдельные физические лица (хакеры) (категория – внешний, уровень возможностей – Н1. Нарушитель, обладающий базовыми возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса).   1. Конкурирующие организации (категория – внешний, уровень возможностей – Н2. Нарушитель, обладающий базовыми повышенными возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - по­луче­ние кон­ку­рен­тных пре­иму­ществ.   1. Разработчики программных, программно-аппаратных средств (категория – внутренний, уровень возможностей – Н3. Нарушитель, обладающий средними возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - по­луче­ние кон­ку­рен­тных пре­иму­ществ;  - внед­ре­ние до­пол­ни­тель­ных фун­кци­ональ­ных воз­можнос­тей в прог­рам­мные или прог­рам­мно-ап­па­рат­ные средс­тва на эта­пе раз­ра­бот­ки;  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия.   1. Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (категория – внешний, уровень возможностей – Н1. Нарушитель, обладающий базовыми возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - по­луче­ние кон­ку­рен­тных пре­иму­ществ;  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия.   1. Поставщики вычислительных услуг, услуг связи (категория – внутренний, уровень возможностей – Н2. Нарушитель, обладающий базовыми повышенными возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - по­луче­ние кон­ку­рен­тных пре­иму­ществ;  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия.   1. Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (категория – внутренний, уровень возможностей – Н2. Нарушитель, обладающий базовыми повышенными возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - по­луче­ние кон­ку­рен­тных пре­иму­ществ;  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия.   1. Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (категория – внутренний, уровень возможностей – Н1. Нарушитель, обладающий базовыми возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия.   1. Авторизованные пользователи систем и сетей (категория – внутренний, уровень возможностей – Н1. Нарушитель, обладающий базовыми возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса);  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия;  - месть за ра­нее со­вер­шенные дей­ствия.   1. Системные администраторы и администраторы безопасности (категория – внутренний, уровень возможностей – Н2. Нарушитель, обладающий базовыми повышенными возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса);  - неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия;  - месть за ра­нее со­вер­шенные дей­ствия.   1. Бывшие (уволенные) работники (пользователи) (категория – внешний, уровень возможностей – Н1. Нарушитель, обладающий базовыми возможностями)   Цели:  - по­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы;  - месть за ра­нее со­вер­шенные дей­ствия. |
| 6.2. | Основные угрозы безопасности информации или обоснование их неактуальности | **Актуальные угрозы безопасности информации:**  УБИ.004: Угроза аппаратного сброса пароля BIOS;  УБИ.006: Угроза внедрения кода или данных;  УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации;  УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS;  УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;  УБИ.013: Угроза деструктивного использования декларированного функционала BIOS;  УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователями;  УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути;  УБИ.018: Угроза загрузки нештатной операционной системы;  УБИ.019: Угроза заражения DNS-кеша;  УБИ.022: Угроза избыточного выделения оперативной памяти;  УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы;  УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации;  УБИ.028: Угроза использования альтернативных путей доступа к ресурсам;  УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию;  УБИ.031: Угроза использования механизмов авторизации для повышения привилегий;  УБИ.033: Угроза использования слабостей кодирования входных данных;  УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными;  УБИ.036: Угроза исследования механизмов работы программы;  УБИ.037: Угроза исследования приложения через отчёты об ошибках;  УБИ.041: Угроза межсайтового скриптинга;  УБИ.045: Угроза нарушения изоляции среды исполнения BIOS;  УБИ.049: Угроза нарушения целостности данных кеша;  УБИ.051: Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;  УБИ.053: Угроза невозможности управления правами пользователей BIOS;  УБИ.061: Угроза некорректного задания структуры данных транзакции;  УБИ.062: Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;  УБИ.063: Угроза некорректного использования функционала программного и аппаратного обеспечения;  УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;  УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;  УБИ.069: Угроза неправомерных действий в каналах связи;  УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;  УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;  УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;  УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;  УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;  УБИ.086: Угроза несанкционированного изменения аутентификационной информации;  УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS;  УБИ.088: Угроза несанкционированного копирования защищаемой информации;  УБИ.089: Угроза несанкционированного редактирования реестра;  УБИ.090: Угроза несанкционированного создания учётной записи пользователя;  УБИ.091: Угроза несанкционированного удаления защищаемой информации;  УБИ.093: Угроза несанкционированного управления буфером;  УБИ.094: Угроза несанкционированного управления синхронизацией и состоянием;  УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб;  УБИ.099: Угроза обнаружения хостов;  УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации;  УБИ.103: Угроза определения типов объектов защиты;  УБИ.104: Угроза определения топологии вычислительной сети;  УБИ.107: Угроза отключения контрольных датчиков;  УБИ.109: Угроза перебора всех настроек и параметров приложения;  УБИ.113: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;  УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации;  УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети;  УБИ.121: Угроза повреждения системного реестра;  УБИ.123: Угроза подбора пароля BIOS;  УБИ.124: Угроза подделки записей журнала регистрации событий;  УБИ.128: Угроза подмены доверенного пользователя;  УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS;  УБИ.130: Угроза подмены содержимого сетевых ресурсов;  УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»;  УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;  УБИ.144: Угроза программного сброса пароля BIOS;  УБИ.145: Угроза пропуска проверки целостности программного обеспечения;  УБИ.152: Угроза удаления аутентификационной информации;  УБИ.153: Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;  УБИ.155: Угроза утраты вычислительных ресурсов;  УБИ.156: Угроза утраты носителей информации;  УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;  УБИ.158: Угроза форматирования носителей информации;  УБИ.159: Угроза «форсированного веб-браузинга»;  УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;  УБИ.162: Угроза эксплуатации цифровой подписи программного кода;  УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов;  УБИ.168: Угроза «кражи» учётной записи доступа к сетевым сервисам;  УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;  УБИ.172: Угроза распространения «почтовых червей»;  УБИ.174: Угроза «фарминга»;  УБИ.175: Угроза «фишинга»;  УБИ.177: Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;  УБИ.178: Угроза несанкционированного использования системных и сетевых утилит;  УБИ.179: Угроза несанкционированной модификации защищаемой информации;  УБИ.182: Угроза физического устаревания аппаратных компонентов;  УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент;  УБИ.191: Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;  УБИ.192: Угроза использования уязвимых версий программного обеспечения;  УБИ.205: Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты;  УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники;  УБИ.209: Угроза несанкционированного доступа к защищаемой памяти ядра процессора;  УБИ.211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем.  В объекте КИИ не используются технологии беспроводного доступа, технологии виртуализации, технологии удаленного рабочего стола, технологии удаленного администрирования, технологии удаленного внеполосного доступа, технологии веб-доступа, технологии передачи речи, технологии передачи видеоинформации, технология больших данных, мобильные технические средства, одноразовые пароли, электронная почта, суперкомпьютеры, числовое программное обеспечение, грид системы. В связи с этим угрозы, реализуемые посредством данных технологий, не рассматриваются. |

1. 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 | Отказ в обслуживании; Модификация (подмена) данных; Нарушение функционирования технических средств |

1. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости

|  |  |  |
| --- | --- | --- |
| 8.1. | Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий | III |
| 8.2. | Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту | 1. Социальная значимость: 2. Причинение ущерба жизни и здоровью людей (человек): 1. Категория III. 3. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые:    1. на территории, на которой возможно нарушение обеспечения жизнедеятельности населения: неприменимо. Категория не присвоена.    2. по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек): неприменимо. Категория не присвоена. 4. Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:    1. на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг): неприменимо. Категория не присвоена.    2. по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек): неприменимо. Категория не присвоена. 5. Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек): неприменимо. Категория не присвоена. 6. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов): неприменимо. Категория не присвоена. 7. Политическая значимость: 8. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): неприменимо. Категория не присвоена. 9. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации: неприменимо. Категория не присвоена. 10. Экономическая значимость: 11. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период): неприменимо. Категория не присвоена. 12. Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период): неприменимо. Категория не присвоена. 13. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений): неприменимо. Категория не присвоена. 14. Экологическая значимость: 15. Вредные воздействия на окружающую среду, оцениваемые:     1. на территории, на которой окружающая среда может подвергнуться вредным воздействиям: неприменимо. Категория не присвоена.     2. по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек): неприменимо. Категория не присвоена. 16. Значимость для обеспечения обороны страны, безопасности государства и правопорядка: 17. Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра: неприменимо. Категория не присвоена. 18. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое:     1. в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции): неприменимо. Категория не присвоена.     2. в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции): неприменимо. Категория не присвоена. 19. Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов): неприменимо. Категория не присвоена. |
| 8.3. | Обоснование полученных значений по каждому из рассчитываемых критериев значимости или информация о неприменимости показателя к объекту | 1. Социальная значимость: 2. Причинение ущерба жизни и здоровью людей (человек):   Медицинским персоналом осуществляется ежедневный регламентированный мониторинг работоспособности медицинского оборудования, входящего в состав объекта КИИ, на основании чего определено усредненное время, требуемое для выявления и устранения последствий компьютерной атаки на объект КИИ: 24 часа. Среднее количество пациентов, обслуживаемое медицинским оборудованием, входящим в состав объекта КИИ, в течение одного рабочего дня: 1 человек. Исходя из расчетов и полученных данных определено максимальное количество человек, жизни и здоровью которых может быть причинен ущерб: 1 человек.   1. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые:    1. на территории, на которой возможно нарушение обеспечения жизнедеятельности населения:   Объект КИИ не осуществляет управление, контроль и мониторинг процессов, относящихся к объектам обеспечения жизнедеятельности населения.   * 1. по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек):   Объект КИИ не осуществляет управление, контроль и мониторинг процессов, относящихся к объектам обеспечения жизнедеятельности населения.   1. Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:    1. на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг):   Объект КИИ не осуществляет управление, контроль и мониторинг процессов объектов транспортной инфраструктуры.   * 1. по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек):   Объект КИИ не осуществляет управление, контроль и мониторинг процессов объектов транспортной инфраструктуры.   1. Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек):   Объект КИИ не является информационно-телекоммуникационной сетью и не осуществляет управление, контроль и мониторинг процессов, обеспечивающую функционирование сетей связи.   1. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов):   Объект КИИ не является системой, оказывающей государственные услуги и не осуществляет управление, контроль и мониторинг процессов, обеспечивающих предоставление государственных услуг.   1. Политическая значимость: 2. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия):   Субъект КИИ не является государственным органом.   1. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации:   Субъект КИИ не является государственным органом.   1. Экономическая значимость: 2. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период):   Субъект КИИ не является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием.   1. Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период):   Налоговые и неналоговые отчисления организацией в федеральный бюджет несоизмеримо малы в сравнении с доходами федерального бюджета.   1. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений):   Субъект КИИ не является системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка.   1. Экологическая значимость: 2. Вредные воздействия на окружающую среду, оцениваемые:    1. на территории, на которой окружающая среда может подвергнуться вредным воздействиям:   Объект КИИ не оказывает управляющие воздействия на автоматизируемый процесс и не оказывает влияние на возникновение аварийной ситуации на объекте.   * 1. по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек):   Объект КИИ не оказывает управляющие воздействия на автоматизируемый процесс и не оказывает влияние на возникновение аварийной ситуации на объекте.   1. Значимость для обеспечения обороны страны, безопасности государства и правопорядка: 2. Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра:   Объект КИИ не является частью (элементом) пункта управления (ситуационным центром) и не осуществляет управление, контроль и мониторинг процессов, обеспечивающих функционирование какого-либо пункта управления (ситуационного центра).   1. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое:    1. в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции):   Объект КИИ не обеспечивает выполнение, управление, контроль и мониторинг государственного оборонного заказа.   * 1. в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции):   Объект КИИ не обеспечивает выполнение, управление, контроль и мониторинг государственного оборонного заказа.   1. Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов):   Объект КИИ не является информационной системой в области обеспечения обороны страны, безопасности государства и правопорядка |

1. 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) | * АУД.1 Инвентаризация информационных ресурсов * ОЦЛ.4 Контроль данных, вводимых в информационную (автоматизированную) систему * ЗТС.2 Организация контролируемой зоны; * ЗТС.3 Управление физическим доступом; * ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр; * ЗТС.5 Защита от внешних воздействий * ЗИС.2 Защита периметра информационной (автоматизированной) системы * УКФ.2 Управление изменениями * ДНС.2 Обучение и отработка действий персонала в нештатных ситуациях * ИПО.1 Информирование персонала об угрозах безопасности информации и о правилах безопасной работы; * ИПО.2 Обучение персонала правилам безопасной работы |
| 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 | * УПД.10 Блокирование сеанса доступа пользователя при неактивности * ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения; * ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения * ОЦЛ.4 Контроль данных, вводимых в информационную (автоматизированную) систему * ЗТС.2 Организация контролируемой зоны; * ЗТС.3 Управление физическим доступом; * ЗТС.5 Защита от внешних воздействий * ЗИС.2 Защита периметра информационной (автоматизированной) системы * УКФ.2 Управление изменениями * ДНС.5 Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций |

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.