Утв. приказом ФСТЭК России

от 22 декабря 2017 г. № 236

*(в ред. от 21 марта 2019 г.)*

**Сведения о результатах присвоения объекту критической**

**информационной инфраструктуры одной из категорий значимости**

**либо об отсутствии необходимости присвоения ему**

**одной из таких категорий**

Ограничительная пометка  
или гриф секретности  
(при необходимости)

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) | Система управления городским транспортом  Система управления ЖКХ  Электронная приемная для граждан  Взаимодействие с ГАС «Управление»  Базы данных (ПДн сотрудников, граждан, жильцов) |
| 1.2 | Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта | Поселок N, ул. Центральная, д. 1 (главный офис муниципального управления) |
| 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» | Транспортная инфраструктура, ЖКХ, государственное управление (п. 8 ст. 2 ФЗ-187 |
| 1.4. | Назначение объекта | Обеспечение функционирования городского транспорта, управление ЖКХ, обработка обращений граждан, взаимодействие с государственными системами |
| 1.5. | Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть) | Информационные системы (ИС), автоматизированные системы управления (АСУ) |
| 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) | Клиент-серверная система (СУБД MySQL, PostgreSQL).  Распределенная система управления (GPS-трекинг транспорта). |

2. Сведения о субъекте критической информационной инфраструктуры

|  |  |  |
| --- | --- | --- |
| 2.1. | Наименование субъекта | МУНИЦИПАЛЬНОЕ УПРАВЛЕНИЕ ПОСЕЛКОМ N |
| 2.2. | Адрес местонахождения субъекта | Поселок N, ул. Центральная, д. 1. |
| 2.3. | Должность, фамилия, имя, отчество (при наличии) руководителя субъекта | Директор муниципального управления — Иванов Иван Иванович. |
| 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 | Специалист по ИБ — Петров Петр Петрович. |
| 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) | Отдел информационной безопасности.   * Руководитель: Петров П.П. * Телефон: +7 (XXX) XXX-XX-XX. * Email: [security@munposelok-n.ru](mailto:security@munposelok-n.ru). |
| 2.6. | ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта | ИНН субъекта: 7701123456.  КПП: 770101001. |

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 | Государственная сеть общего пользования (транспортная система).  Локальная сеть (ЖКХ, базы данных).  Публичная сеть (электронная приемная). |
| 3.2. | Наименование оператора связи и (или) провайдера хостинга | ОАО «Ростелеком», ПАО «МТС», ФГУП «Госсвязь». |
| 3.3. | Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Передача данных GPS-трекинга, управление коммунальными услугами, обработка обращений граждан, интеграция с ГАС «Управление». |
| 3.4. | Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия | Проводные каналы (оптоволокно), защищенные VPN-туннели, HTTPS. |

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |  |
| --- | --- | --- |
| 4.1. | Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект | МУНИЦИПАЛЬНОЕ УПРАВЛЕНИЕ ПОСЕЛКОМ N. |
| 4.2. | Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект | Поселок N, ул. Центральная, д. 1. |
| 4.3. | Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты) | Серверное оборудование (5 шт.), телекоммуникационное оборудование (маршрутизаторы, коммутаторы). |
| 4.4. | ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта | ИНН: 7701123456, КПП: 770101001. |

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 | Серверы: 5 шт.  Пользовательские компьютеры: 10 шт.  Телекоммуникационное оборудование: маршрутизаторы (1 шт.), коммутаторы (4 шт.). |
| 5.2. | Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)) | ОС: Windows Server, Linux.  Средства виртуализации: VMware. |
| 5.3. | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем) | Система управления транспортом, ПО для ЖКХ, веб-интерфейс электронной приемной. |
| 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 | Межсетевые экраны, антивирусное ПО (Kaspersky Endpoint Security), шифрование TLS. |

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 | Внешние: Хакеры, киберпреступники (мотивация — дестабилизация работы).  Внутренние: Сотрудники с избыточными правами (ошибки или умышленные действия). |
| 6.2. | Основные угрозы безопасности информации или обоснование их неактуальности | DDoS-атаки, утечки ПДн, несанкционированный доступ к системам управления. |

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 | Отказ в обслуживании транспорта/ЖКХ.  Утечка персональных данных (СНИЛС, паспорта).  Нарушение работы ГАС «Управление». |

8. 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 | Система управления транспортом: Высокая.  Система управления ЖКХ: Средняя.  Электронная приемная: Средняя. |
| 8.2. | Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту | Социальная значимость: Угроза жизни >10 000 человек (транспорт).  Экономическая значимость: Потери бюджета до 15% (ЖКХ). |
| 8.3. | Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту | Транспортная система влияет на безопасность населения, ЖКХ — на жизнедеятельность. |

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) | Контроль доступа к серверным помещениям.  Разработка регламентов по обработке ПДн. |
| 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 | Двухфакторная аутентификация.  Регулярное обновление ПО, резервное копирование данных. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| (наименование должности руководителя субъекта  критической информационной инфраструктуры или  уполномоченного им лица) |  | (подпись) |  | (инициалы, фамилия) |

М. П.

(при наличии печати)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| « |  | » |  | 20 |  | г. |