# Пример заполненного акта категорирования объекта КИИ

УТВЕРЖДАЮ

<Главный врач

Наименование МО

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ФИО

«\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2019 г.

**АКТ
категорирования объекта КИИ**

|  |  |  |
| --- | --- | --- |
| Состав комиссии | Должность  | ФИО |
|  |  |  |
| Председатель комиссии | Должность  | ФИО |
| Члены комиссии | Должность  | ФИО |
|  | Должность  | ФИО |
|  | Должность  | ФИО |
|  | Должность  | ФИО |
|  | Должность  | ФИО |

Комиссия, рассмотрев следующие исходные данные:

1. Сведения об объекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование объекта  | Медицинская информационная система  |
| Адреса размещения объекта | г. Москва, ул. г. Москва, \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Сфера (область) деятельности, в которой функционирует объект | Сфера здравоохранения |
| Назначение объекта  | Автоматизация информационных процессов, сопровождающих лечебно-диагностическую, хозяйственную и управленческую деятельность |
| Тип объекта  | Информационная система |
| Архитектура объекта  | Клиент-серверная система |

1. Сведения о субъекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование субъекта  | ГБУЗ «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ДЗМ» |
| Адрес местонахождения субъекта  | г. Москва, ул. г. Москва, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Должность, фамилия, имя, отчество (при наличии) руководителя субъекта  | Главный врач  |
| Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов  | Заместитель главного врача |
| 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)  | Отдел Информационных технологий Начальник отдела информационных технологий  |
| ИНН субъекта и КПП его обособленных подразделений  | ИНН - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_КПП- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

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  | Закрытая внутренняя локально вычислительная сеть, без подключения к внешним линиям связи. |
| Наименования оператора связи  | Внутренняя информационно-коммуникационная сеть |
| Цель взаимодействия с сетью электросвязи  | Передача данных от клиента к серверу |
| Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия  | Проводной, TCP/IP |

1. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование лица, эксплуатирующего объект  | ГБУЗ «\_\_\_\_\_\_\_\_\_\_\_\_\_» |
| Адрес местонахождения лица, эксплуатирующего объект  | г. Москва, ул. г. Москва, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Элемент (компонент) объекта, который эксплуатируется лицом  | Объект целиком эксплуатируется субъектом |
| ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта | ИНН - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_КПП - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

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  | * Серверы: 1 шт.
* Пользовательские компьютеры – 600 шт.
* Отказоустойчивая система хранения данных
* Ленточная библиотека
 |
| Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)  | Windows 7, Windows 10Windows Server 2016  |
| Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем) | Microsoft SQL server 2016 |
| Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименование 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  | * АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат соответствия СФ/СЗИ-0100, №3025, Kaspersky Security Centre 10 сертификат соответствия СФ/СЗИ-0098, СФ/019-3113, №3155, СФ/019-3468

‒ ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД |

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  | [Приложение 5](#_Приложение_5) (Распечатать и приложить к акту категорирования объекта КИИ) |
| Основные угрозы безопасности информации или обоснование их неактуальности  | [Приложение 6](#_Приложение_6) (Распечатать и приложить к акту категорирования объекта КИИ) |

1. Возможные последствия в случае возникновения компьютерных инцидентов инфраструктуры

|  |  |
| --- | --- |
| 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. |

1. Категория значимости, которая присвоена объекту критической информационной инфраструктуры.

|  |  |
| --- | --- |
| Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий | Без категории |
| Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту | См. пункт Результаты оценки показателей (ниже по тексту) 127- ПП  |
| Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту | См. пункт Результаты оценки показателей (ниже по тексту) 127 - ПП |

Результаты оценки показателей:

|  |  |  |  |
| --- | --- | --- | --- |
| №  | Показатель  | Выбранное значение  | Обоснование[[1]](#footnote-1)  |
| *I. Социальная значимость*  |
| 1  | Причинение ущерба жизни и здоровью людей (человек)  | Не применимо | нарушение функционирования объекта не оказывает влияние на возможность причинения ущерба жизни и здоровью людей. |

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

|  |  |
| --- | --- |
| Организационные меры по обеспечению безопасности объекта  | Объект КИИ не является значимым - обязательных мер не установлено |
| Технические меры по обеспечению безопасности объекта | Объект КИИ не является значимым - обязательных мер не установлено |

Настоящий акт составлен в единственном экземпляре.

|  |  |  |  |
| --- | --- | --- | --- |
| Состав комиссии | Должность  | ФИО | Подпись |
|  |  |  |  |
| Председатель комиссии | Должность  | ФИО | Подпись |
| Члены комиссии | Должность  | ФИО | Подпись |
|  | Должность  | ФИО | Подпись |
|  | Должность  | ФИО | Подпись |
|  | Должность  | ФИО | Подпись |
|  | Должность  | ФИО | Подпись |

В случае если будет выявлена категория, в течении десяти рабочих дней, необходимо направить во ФСТЭК России ([Приложение 4](#_Приложение_4_–) – форма уведомления ФСТЭК России «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» в течении десяти рабочих дней направляет сведения о результатах категорирования. Акт категорирования в ФСТЭК не отпраляется.

В течении тридцати дней ФСТЭК России проверяет соблюдение порядка и правильности категорирования и в случае положительного заключения, вносит сведения в реестр значимых объектов КИИ с последующим уведомлением субъекта КИИ в десятидневный срок.

Предоставлять информацию об отсутствии в организации объектов критической информационной инфраструктуры, или о том, что организация не является субъектом КИИ в ФСТЭК России не требуется.

1. Информация приведена в качестве примера.

В соответствии с разъяснениями ФСТЭК России, в обосновании каждой оценки необходимо предоставлять полную и достоверную информацию, на основании которой можно будет проверить/подтвердить сделанный вывод и присвоении категории. То есть уточнить как делался расчет, какие компенсационные меры учитывали и почему и т.д. [↑](#footnote-ref-1)