**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**По выполнению требований федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры**

**Российской Федерации» в Медицинских организациях**

**г. Нижний Новгород**

**2019**

Оглавление

[1. Термины и определения 3](#_Toc3365329)

[2. Перечень нормативных документов, на которые необходимо ориентироваться при работе с КИИ 4](#_Toc3365330)

[3. Общие положения 5](#_Toc3365331)

[4. Этапы и мероприятия по обеспечению безопасности значимых объектов КИИ 7](#_Toc3365332)

[5. Мероприятия этапа «Аудит и категорирование» 8](#_Toc3365333)

[6. Создание комиссии по категорированию 10](#_Toc3365334)

[7. Определение процессов 11](#_Toc3365335)

[8. Выявление критических процессов 12](#_Toc3365336)

[9. Определение объектов КИИ 13](#_Toc3365337)

[10. Сбор исходных данных об объекте КИИ 15](#_Toc3365338)

[11. Оценка значимости объектов КИИ 17](#_Toc3365339)

[Приложение 1 – форма перечня объектов КИИ 21](#_Toc3365340)

[Приложение 2 – форма письма для отправки во ФСТЭК России 22](#_Toc3365341)

[Приложение 3 – форма письма для отправки в Министерство здравоохранения Нижегородской области 23](#_Toc3365342)

[Приложение 4 – форма акта категорирования объекта КИИ 24](#_Toc3365343)

[Приложение 5 – форма уведомления ФСТЭК России о сведениях об объектах КИИ 28](#_Toc3365344)

## Термины и определения

Критическая информационная инфраструктура (КИИ) - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов (Далее - **КИИ**).

Объектами КИИ являются:

* информационные системы (**ИС**);
* информационно-телекоммуникационные сети (**ИТКС**);
* автоматизированные системы управления (**АСУ**).

К субъектам КИИ относятся государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Сведения о том, является ли организация субъектом КИИ, можно получить в следующих источниках:

* Общероссийский классификатор видов экономической деятельности;
* Лицензии и иные разрешительные документы на различные виды деятельности;
* Уставы, положения организаций;
* Другие источники.

## Перечень нормативных документов, на которые необходимо ориентироваться при работе с КИИ

1. Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ).
2. Постановление Правительства РФ №127 от 08.02.2019 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (ПП 127).
3. Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
5. Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
6. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

## Общие положения

В соответствии с 187-ФЗ «к субъектам критической информационной инфраструктуры относятся государственные органы и учреждения, а также российские юридические лица и/или индивидуальные предприниматели которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления».

У каждого субъекта КИИ есть объекты КИИ:

* информационные системы;
* автоматизированные системы управления технологическими процессами;
* информационно-телекоммуникационные сети.

Объекты КИИ - это совокупность средств вычислительной техники, информационных систем, средств телекоммуникации (благодаря которым объект КИИ функционирует). Объекты КИИ обеспечивают функционирование управленческих, технологических, производственных, финансово-экономических и иных процессов субъектов КИИ.

Если разделить работу с КИИ на крупные шаги, то можно получить следующий порядок:

Первый шаг. Необходимо создать внутреннюю комиссию по категорированию и определить состав участников из наиболее компетентных специалистов по вашим бизнес-процессам. Почему делается акцент на бизнес-процессы и уровни компетенции участников? Только «владелец» бизнес-процесса знает все нюансы, которые могут привести к их нарушению и последующим негативным последствиям. Этот владелец или компетентное уполномоченное лицо должен быть в составе комиссии для присвоения правильной категории значимости процессу.

Второй шаг. На этом этапе собираются исходные данные, проводится предпроектное обследование и на основании полученных данных, комиссия принимает решение о наличии перечня объектов КИИ, подлежащих категорированию и присваивает категорию значимости. Согласно ПП 127, выделяют три категорий значимости три, первая самая высокая.

 Категории значимости присваиваются исходя из показателей критериев значимости, которых пять:

* социальная;
* политическая;
* экономическая;
* экологическая;
* значимость для обеспечения обороны страны, безопасности государства и правопорядка.

На этом шаге есть один нюанс, после утверждения перечня объектов КИИ подлежащих категорированию, субъект КИИ в течении пяти дней обязан известить об этом ФСТЭК России. С этого момента на проведение процедур категорирования отводится максимум один год. Если объект КИИ не подпадает под один из показателей критериев значимости, то у него отсутствует необходимость присвоения категории значимости, но тем не менее предприятие является субъектом КИИ у которого отсутствуют критически значимые объекты КИИ.

Результатом второго шага является «[Акт категорирования объекта КИИ](https://www.ec-rs.ru/%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%B5%D1%86%20%D0%B0%D0%BA%D1%82%D0%B0%20%D0%BA%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0%20%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80....pdf)», который подписывается членами комиссии и утверждается руководителем субъекта КИИ. Акт должен содержать полные сведения об объекте КИИ и хранится субъектом до последующего пересмотра критериев значимости. С момента подписания акта, субъект КИИ в течении десяти дней направляет сведения о результатах категорирования по [утверждённой форме](http://regulation.gov.ru/projects#npa=76034) в ФСТЭК России (на момент написания статьи форма на стадии согласования окончательного варианта). 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.

Третий шаг. Заключается в выполнении требований по обеспечению безопасности значимых объектов КИИ. Ключевые стадии по обеспечению безопасности объектов КИИ:

* разработка технического задания;
* разработка модели угроз информационной безопасности;
* разработка технического проекта;
* разработка рабочей документации;
* ввод в действие.

## Этапы и мероприятия по обеспечению безопасности значимых объектов КИИ

| №  п/п | Наименование этапа | Состав мероприятий |
| --- | --- | --- |
| 1 | 2 |
| 1 | Аудит  и категорирование | Определение процессов организации и выявление критический процессов. Определение и формирование перечня объектов КИИ. Создание комиссии по категорированию. Сбор исходных данных об объекте КИИ. Анализ угроз. Оценка значимости объектов КИИ. Присвоение категории значимости объектов КИИ и уведомление регулятора. |
| 2 | Установление требований  к обеспечению безопасности значимого объекта | Подготовка технического задания на подсистему безопасности значимого объекта. |
| 3 | Разработка организационных  и технических мер  по обеспечению безопасности значимого объекта | Анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии). Проектирование подсистемы безопасности значимого объекта. Разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности). |
| 4 | Внедрение организационных  и технических мер  по обеспечению безопасности значимого объекта  и ввод его в действие | Установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств. Разработка организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта. Внедрение организационных мер по обеспечению безопасности значимого объекта. Предварительные испытания значимого объекта и его подсистемы безопасности. Опытная эксплуатация значимого объекта и его подсистемы безопасности. Анализ уязвимостей значимого объекта и принятие мер по их устранению. Приемочные испытания значимого объекта и его подсистемы безопасности. |
| 5 | Обеспечение безопасности значимого объекта  в ходе его эксплуатации | Планирование мероприятий по обеспечению безопасности значимого объекта. Анализ угроз безопасности информации в значимом объекте и последствий от их реализации. Управление (администрирование) подсистемой безопасности значимого объекта. Управление конфигурацией значимого объекта и его подсистемой безопасности. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта. Обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта. Информирование и обучение персонала значимого объекта. Контроль за обеспечением безопасности значимого объекта. |
| 6 | Обеспечение безопасности значимого объекта при выводе его  из эксплуатации | Архивирование информации, содержащейся в значимом объекте. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации. Уничтожение данных об архитектуре и конфигурации значимого объекта. |

## Мероприятия этапа «Аудит и категорирование»

В рамках настоящего документа рассматриваются мероприятия первого этапа – «Аудит и категорирование»:

| №  п/п | Наименование мероприятия | Состав работ |
| --- | --- | --- |
| 1 | 2 |
| 1 | Создание комиссии по категорированию | Необходимо создать комиссию по категорированию объектов. |
| 2 | Определение процессов | Необходимо определить управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ. |
| 3 | Выявление критических процессов | Необходимо выявить процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка. |
| 4 | Определение объектов КИИ | Необходимо определить объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. |
| 5 | Формирование перечня объектов КИИ | Необходимо сформировать перечень объектов КИИ, подлежащих категорированию. |
| 6 | Сбор исходных данных об объекте КИИ | Необходимо собрать следующие сведения:  а) сведения об объекте КИИ (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи);  б) процессы, которые обеспечивают управленческие, технологические, производственные, финансово- экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ;  в) состав информации, обрабатываемой объектами КИИ, сервисы по управлению, контролю или мониторингу, предоставляемые объектами КИИ;  г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект КИИ (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);  д) сведения о взаимодействии объекта КИИ с другими объектами КИИ и (или) о зависимости функционирования объекта КИИ от других таких объектов. |
| 7 | Анализ угроз | Необходимо:  выявить группы угроз безопасности информации в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа;  рассмотреть возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;  проанализировать угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ. |
| 8 | Оценка значимости объектов КИИ | Необходимо провести оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ |
| 9 | Присвоение категории значимости объектов КИИ | Необходимо присвоить каждому из объектов КИИ одну из категорий значимости, либо обосновать принятие решения об отсутствии необходимости присвоения им одной из категорий значимости |
| 10 | Подготовка сведений о категорировании объектов КИИ | Необходимо подготовить документ «Сведения о категорировании объектов КИИ» в соответствии с требованиями Приказа ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» |

В следующих разделах настоящего документа рассматриваются вышеописанные мероприятия из пунктов – 1, 2, 3, 4, 6, 8 подробнее.

## Создание комиссии по категорированию

Для проведения категорирования решением руководителя субъекта КИИ создается комиссия по категорированию, в состав которой включаются:

* руководитель субъекта КИИ или уполномоченное им лицо;
* работники субъекта КИИ, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;
* работники субъекта КИИ, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ;
* работники подразделения по защите государственной тайны субъекта КИИ (в случае, если объект КИИ обрабатывает информацию, составляющую государственную тайну);
* работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

Следует отметить, что в состав комиссии по категорированию могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с государственными органами и российскими юридическими лицами.

Комиссию по категорированию возглавляет руководитель субъекта КИИ или уполномоченное им лицо.

Комиссия по категорированию в ходе своей работы:

* определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;
* выявляет наличие критических процессов у субъекта КИИ;
* выявляет объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;
* рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;
* анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
* оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
* устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

## Определение процессов

Необходимо определить управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

Перечень процессов (пример):

1. Оказание медицинских услуг и медицинской помощи
   1. Стационарная медицинская помощь
   2. Амбулаторная медицинская консультативная и лечебная помощь
   3. Восстановительное лечение
   4. Диагностическая медицинская помощь
   5. Высокотехнологическая медицинская помощь
2. Проведение исследований, клинических испытаний, осмотров
3. Фармацевтическая деятельность
4. Деятельность по обороту наркотических средств и психотропных веществ
5. Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия)
6. Сбор, хранение и реализация донорской крови
7. Организация общественного питания
8. Розничная торговля товарами личной гигиены и общего потребления
9. Услуги длительного пребывания пациентов / госпитализации (в т.ч. палаты повышенной комфортности)
10. Проведение конференций, семинаров и иных ученых мероприятий
11. Осуществление автотранспортных услуг
12. Управление персоналом
    1. Подбор персонала
    2. Кадровый учет
    3. Расчёт и начисление заработной платы
    4. Организация командировок
    5. Обучение работников
13. Бухгалтерский учет
14. Контрольно-пропускной режим
15. Заключение договоров с контрагентами
16. Обслуживание ИТ-инфраструктуры
17. Обслуживание инженерных систем (Электроснабжение; Система отопления; Водопровод; Канализация; Вентиляция и кондиционирование; Системы пожаробезопасности)
18. Работа с обращениями клиентов
19. Претензионная и судебная работа

## Выявление критических процессов

Необходимо выявить процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование процесса | Негативные последствия | | | | |
| Соц. | Полит. | Эконом. | Эколог. | Оборон. |
| 1. 1. | Оказание медицинских услуг и медицинской помощи | + |  |  |  |  |
|  | Проведение исследований, клинических испытаний, осмотров | + |  |  |  |  |
|  | Фармацевтическая деятельность | + |  |  |  |  |
|  | Деятельность по обороту наркотических средств и психотропных веществ | + |  |  |  |  |
|  | Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия) | + |  |  |  |  |
|  | Сбор, хранение и реализация донорской крови | + |  |  |  |  |
|  | Организация общественного питания |  |  |  |  |  |
|  | Розничная торговля товарами личной гигиены и общего потребления |  |  |  |  |  |
|  | Услуги длительного пребывания пациентов / госпитализации / стационар (в т.ч. палаты повышенной комфортности) | + |  |  |  |  |
|  | Проведение конференций, семинаров и иных ученых мероприятий |  |  |  |  |  |
|  | Осуществление автотранспортных услуг (медицинская транспортировка) | + |  |  |  |  |
|  | Управление персоналом |  |  |  |  |  |
|  | Бухгалтерский учет |  |  | + |  |  |
|  | Контрольно-пропускной режим |  |  |  |  |  |
|  | Заключение договоров с контрагентами |  |  | + |  |  |
|  | Обслуживание ИТ-инфраструктуры |  |  |  |  |  |
|  | Обслуживание инженерных систем (пожарная сигнализация, электропитание) | + |  |  |  |  |
|  | Работа с обращениями клиентов |  |  |  |  |  |
|  | Претензионная и судебная работа |  |  |  |  |  |

## Определение объектов КИИ

Определение объектов КИИ (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления), которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов:

* Оказание медицинских услуг и медицинской помощи
* Проведение исследований, клинических испытаний, осмотров
* Фармацевтическая деятельность
* Деятельность по обороту наркотических средств и психотропных веществ
* Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия)
* Сбор, хранение и реализация донорской крови
* Услуги длительного пребывания пациентов / госпитализации / стационар (в т.ч. палаты повышенной комфортности)
* Осуществление автотранспортных услуг (медицинская транспортировка)
* Бухгалтерский учет
* Заключение договоров с контрагентами
* Обслуживание инженерных систем (пожарная сигнализация, электропитание)

Перечень объектов, подлежащий категорированию (примеры):

Информационные системы:

* «Электронная очередь»
* «АИС Поликлиника»
* «АИС Стационар»
* Регистры больных
* АРМ РМИС НО
* АРМ МИС МО
* АРМ РИСАР
* ИПРА

Информационно-телекоммуникационные сети:

* защищенная сеть МО

Автоматизированные системы управления:

* Автоматизированная система оперативного управления диспетчерской службой скорой медицинской помощи
* АСУ пожаротушением
* АСУ рентген аппаратами
* АСУ томографом
* АСУ лучевой терапия

В перечень КИИ должны входить только те системы, которые имеют прямо отношению к типу деятельности организации.

Должны быть указаны объекты информационной инфраструктуры находящиеся в МО на праве собственности или аренды.

Оборудование типа – Рентгеновский аппарат, МРТ, КТ и т.д. прошедшее регистрацию в Росздравнадзоре относится к медицинским изделиям и также в перечне не указывается.

Формы перечня объектов КИИ в приложении 1 к настоящему документу.

Форма уведомления ФСТЭК России о перечне объектов КИИ в приложении 2 к настоящему документу.

Форма уведомления Министерства здравоохранения Нижегородской области о перечне объектов КИИ в приложении 3 к настоящему документу.

**Сначала необходимо перечень согласовать с МЗ НО и затем направить в адрес ФСТЭК РФ.**

## Сбор исходных данных об объекте КИИ

На этом этапе необходимо собрать:

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

б) процессы, инфраструктуры; указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной

в) состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);

д) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов/

Объект (пример):

* АРМ РМИС НО – автоматизированное рабочее место подключенное к региональной медицинской информационной системе Нижегородской области

1. Сведения об объекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование объекта: | АРМ РМИС НО |
| Адреса размещения объекта: | Нижегородская область, г. , ул. |
| Сфера (область) деятельности, в которой функционирует объект: | Здравоохранение |
| Назначение объекта | Поддержка процесса управления оказания медицинской помощи населению и повышение качества медицинского обслуживания |
| Критические процессы, которые обеспечиваются объектом | Оказание медицинских услуг и медицинской помощи |
| Архитектура объекта | клиент-серверная систем.  АРМ – Сервер приложений |

2. Сведения о субъекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование субъекта | <Наименование МО> |
| Адрес (местонахождение) субъекта | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения субъекта | Нижегородская область, г. , ул. |
| Руководитель субъекта | Иванов И.И. |
| Лицо, на которое возложены функции обеспечения безопасности объектов6 | Петров П.П. |
| Структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов | АСУ |

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

|  |  |
| --- | --- |
| Категория сети электросвязи | Сеть связи общего пользования, защищенная сеть связи МЗ НО |
| Наименование оператора связи | Ростелеком, Минздрав НО |
| Цель взаимодействия с сетью электросвязи | Оказание услуг, контроль |
| Способ взаимодействия с сетью электросвязи | Проводной доступ, доступ через VPN |

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование лица, эксплуатирующего объект | <Наименование МО> |
| Адрес (местонахождение) лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Элемент (компонент) объекта, который эксплуатируется лицом | Все компоненты |

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

|  |  |
| --- | --- |
| Программно-аппаратные средства | Пользовательские компьютеры, серверы, телекоммуникационное оборудование |
| Общесистемное программное обеспечение | Ubuntu Linux, Windows, ... |
| Прикладное программное обеспечение | РМИС НО |
| Средства защиты информации | ViPNet Client 4, сертификат 12345, ПАК Jacarta, сертификат 12345, Антивирус Kaspersky Endpoint 10, сертификат 12345 |

## Оценка значимости объектов КИИ

Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры

Объект (пример):

* АРМ РМИС НО – автоматизированное рабочее место подключенное к региональной медицинской информационной системе Нижегородской области

Возможные последствия: причинение ущерба жизни и здоровью людей от 1 до 50 человек

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Показатель | | Значение показателя | | | |
| III категория | II категория | I категория | Без категории |
| I. Социальная значимость | | | | |  |
| 1. | Причинение ущерба жизни и здоровью людей (человек) |  |  |  | + |
| 2. | Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые: |  |  |  |  |
|  | а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения; |  |  |  | + |
|  | б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек) |  |  |  |  |
| 3. | Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые: |  |  |  |  |
|  | а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг; |  |  |  | + |
|  | б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек) |  |  |  | + |
| 4. | Прекращение или нарушение функционирования сети связи, оцениваемые: |  |  |  |  |
|  | а) на территории, на которой возможно прекращение или нарушение функционирования сети связи; |  |  |  | + |
|  | б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек) |  |  |  | + |
| 5. | Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов) |  |  |  | + |
| II. Политическая значимость | | | | |  |
| 6. | Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) |  |  |  | + |
| 7. | Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации |  |  |  | + |
| III. Экономическая значимость | | | | |  |
| 8. | Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) 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 прогнозируемого объема годового дохода по всем видам деятельности) |  |  |  | + |
| 9. | Возникновение ущерба бюджетам Российской Федерации, оцениваемого: |  |  |  |  |
|  | а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета); |  |  |  | + |
|  | б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета); |  |  |  | + |
|  | в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета) |  |  |  | + |
| 10. | 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) |  |  |  | + |
| IV. Экологическая значимость | | | | |  |
| 11. | Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые: |  |  |  |  |
|  | а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям; |  |  |  | + |
|  | б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек) |  |  |  | + |
| V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка | | | | |  |
| 12. | Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра |  |  |  | + |
| 13. | Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое: |  |  |  |  |
|  | а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции); |  |  |  | + |
|  | б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции) |  |  |  | + |
| 14. | 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) |  |  |  | + |

Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также 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.

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта КИИ.

Субъект КИИ обеспечивает хранение акта до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости.

Субъект КИИ в течение 10 дней со дня утверждения акта направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ, сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Форма Акта категорирования объекта КИИ в приложении 4 к настоящему документу.

Форма уведомления ФСТЭК России о сведениях об объектах КИИ в приложении 5 к настоящему документу.

## Приложение 1 – форма перечня объектов КИИ

УТВЕРЖДАЮ

<*Должность*>

<*Наименование МО*>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<*ФИО*>

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

**ПЕРЕЧЕНЬ  
объектов критической информационной инфраструктуры   
<*наименование учреждения*>**

| Наименование и назначение объекта КИИ | Планируемый срок категорирования |
| --- | --- |
| **ИС:**  «Электронная очередь»  «АИС Поликлиника»  «АИС Стационар»  Регистры больных  АРМ РМИС НО  АРМ МИС МО  АРМ РИСАР  ИПРА | 1 июля 2019 г. |

|  |  |  |
| --- | --- | --- |
| <Руководитель МО> | <Подпись> | <ФИО> |
| <Наименование МО> |  |  |

## Приложение 2 – форма письма для отправки во ФСТЭК России

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | Начальнику 2 Управления  ФСТЭК России  Шевцову Д.Н.  г. Москва, ул. Старая Басманная, д. 17 |
|  |
|  |
| *О направлении перечня объектов критической информационной инфраструктуры* |
|  |

Уважаемый Дмитрий Николаевич!

В соответствии с требованиями пункта 15 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2019 г. № 127 направляем Вам перечень объектов критической информационной инфраструктуры нашей организации.

| Наименование организации | Сфера деятельности | Наименование и назначение объекта КИИ | Планируемый срок категорирования | Адрес и контакты организации |
| --- | --- | --- | --- | --- |
| <наименование учреждения> | Здравоохранение | **ИС:**  «Электронная очередь»  «АИС Поликлиника»  «АИС Стационар»  Регистры больных  АРМ РМИС НО  АРМ МИС МО  АРМ РИСАР  ИПРА | 1 июля 2019 г. | Руководитель – Иванов И.И.  (098)7654321  [email@mail.ru](mailto:main@kkb0.ru)  Нижегородская область, г. , ул. . |

Согласование проводилось в Министерстве здравоохранения Нижегородской области №\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 2019 г. в Приложении к настоящему письму.

|  |  |  |
| --- | --- | --- |
| <Руководитель МО> | <Подпись> | <ФИО> |
| <Наименование МО> |  |  |

## Приложение 3 – форма письма для отправки в Министерство здравоохранения Нижегородской области

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | Министру здравоохранения Нижегородской области  Шаклунову А. А.  603005, г. Нижний Новгород, ул. Малая Ямская, 78 |
|  |
| *О направлении перечня объектов КИИ* |

Уважаемый Антон Александрович!

В соответствии с требованиями пункта 15 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2019 г. № 127 направляем Вам на согласование предварительный перечень объектов критической информационной инфраструктуры нашей организации.

| Наименование организации | Сфера деятельности | Наименование и назначение объекта КИИ | Планируемый срок категорирования | Адрес и контакты организации |
| --- | --- | --- | --- | --- |
| <наименование учреждения> | Здравоохранение | **ИС:**  «Электронная очередь»  «АИС Поликлиника»  «АИС Стационар»  Регистры больных  АРМ РМИС НО  АРМ МИС МО  АРМ РИСАР  ИПРА | 1 июля 2019 г. | Руководитель – Иванов И.И.  (098)7654321  [email@mail.ru](mailto:main@kkb0.ru)  Нижегородская область, г. , ул. . |

|  |  |  |
| --- | --- | --- |
| <Руководитель МО> | <Подпись> | <ФИО> |
| <Наименование МО> |  |  |

## Приложение 4 – форма акта категорирования объекта КИИ

УТВЕРЖДАЮ

<*Должность*>

<*Наименование МО*>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<*ФИО*>

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

|  |
| --- |
|  |

**АКТ  
категорирования объекта КИИ**

**АДИС**

Состав комиссии:

|  |  |
| --- | --- |
| Председатель комиссии: | <*Должность*><*ФИО*> |
| Члены комиссии: | <*Должность*><*ФИО*> |
|  | <*Должность*><*ФИО*> |
| <*Должность*><*ФИО*> |

Комиссия, рассмотрев следующие исходные данные:

1. Сведения об объекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование объекта: | АРМ РМИС НО |
| Адреса размещения объекта: | Нижегородская область, г. , ул. |
| Сфера (область) деятельности, в которой функционирует объект: | Здравоохранение |
| Назначение объекта | Поддержка процесса управления оказания медицинской помощи населению и повышение качества медицинского обслуживания |
| Критические процессы, которые обеспечиваются объектом | Оказание медицинских услуг и медицинской помощи |
| Архитектура объекта | клиент-серверная систем.  АРМ – Сервер приложений |

2. Сведения о субъекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование субъекта | <Наименование МО> |
| Адрес (местонахождение) субъекта | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения субъекта | Нижегородская область, г. , ул. |
| Руководитель субъекта | Иванов И.И. |
| Лицо, на которое возложены функции обеспечения безопасности объектов6 | Петров П.П. |
| Структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов | АСУ |

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

|  |  |
| --- | --- |
| Категория сети электросвязи | сеть связи общего пользования, защищенная сеть связи МЗ НО |
| Наименование оператора связи | Ростелеком, Минздрав НО |
| Цель взаимодействия с сетью электросвязи | Оказание услуг, контроль |
| Способ взаимодействия с сетью электросвязи | Проводной доступ, доступ через VPN |

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование лица, эксплуатирующего объект | <Наименование МО> |
| Адрес (местонахождение) лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Элемент (компонент) объекта, который эксплуатируется лицом | Все компоненты |

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

|  |  |
| --- | --- |
| Программно-аппаратные средства | пользовательские компьютеры, серверы, телекоммуникационное оборудование |
| Общесистемное программное обеспечение | Ubuntu linux, windows, ... |
| Прикладное программное обеспечение | РМИС |
| Средства защиты информации | ViPNet Client 4, сертификат 12345, ПАК Jacarta, сертификат 12345, Антивирус Kaspersky Endpoint 10, сертификат 12345 |

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

|  |  |
| --- | --- |
| Категория нарушителя | Внешний нарушитель с низким потенциалом |
| Угрозы безопасности информации | Угроза несанкционированного доступа за счет заражения вредоносным кодом  Угроза атак на уровне сети  Угроза удаленного подбора пароля |

7. Возможные последствия в случае возникновения компьютерных инцидентов

|  |  |
| --- | --- |
| Типы компьютерных инцидентов | отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта |
| Возможные последствия от компьютерных инцидентов | причинение ущерба жизни и здоровью людей отсутствует |

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

|  |  |
| --- | --- |
| Категория значимости объекта | Без категории |
| Результаты оценки показателей | причинение ущерба жизни и здоровью людей отсутствует |

9. Организационные и технические меры, необходимые для обеспечения безопасности объекта критической информационной инфраструктуры в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными ФСТЭК России

|  |  |
| --- | --- |
| Организационные меры | установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта |
| Технические меры | идентификация и аутентификация, управление доступом, ограничение программной среды, антивирусная защита, межсетевое экранирование, VPN |

установила информационной системе "АРМ РМИС НО" уровень значимости объекта КИИ - без категории.

Настоящий акт составлен в единственном экземпляре.

|  |  |  |
| --- | --- | --- |
| Председатель комиссии: | <*Должность*><*ФИО*> | |
|  |
| Члены комиссии: | <*Должность*><*ФИО*> |
|  | <*Должность*><*ФИО*> | |
|  | <*Должность*><*ФИО*> | |
|  |  | |

## Приложение 5 – форма уведомления ФСТЭК России о сведениях об объектах КИИ

УТВЕРЖДАЮ

<*Должность*>

<*Наименование МО*>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<*ФИО*>

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

|  |
| --- |
|  |
|  |
| *О сведениях об объекте*  *критической информационной инфраструктуры* | |

Уважаемый Дмитрий Николаевич!

В соответствии с требованиями пункта 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2019 г. № 127 направляем Вам сведения о результатах присвоения категорий значимости объекту критической информационной инфраструктуры.

* 1. Сведения об объекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование объекта: | АРМ РМИС НО |
| Адреса размещения объекта: | Нижегородская область, г. , ул. |
| Сфера (область) деятельности, в которой функционирует объект: | Здравоохранение |
| Назначение объекта | Поддержка процесса управления оказания медицинской помощи населению и повышение качества медицинского обслуживания |
| Критические процессы, которые обеспечиваются объектом | Оказание медицинских услуг и медицинской помощи |
| Архитектура объекта | клиент-серверная систем.  АРМ – Сервер приложений |

* 1. Сведения о субъекте критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование субъекта | <Наименование МО> |
| Адрес (местонахождение) субъекта | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения субъекта | Нижегородская область, г. , ул. |
| Руководитель субъекта | Иванов И.И.. |
| Лицо, на которое возложены функции обеспечения безопасности объектов6 | Петров П.П. |
| Структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов | АСУ |

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

|  |  |
| --- | --- |
| Категория сети электросвязи | сеть связи общего пользования, защищенная сеть связи МЗ НО |
| Наименование оператора связи | Ростелеком, Минздрав НО |
| Цель взаимодействия с сетью электросвязи | Оказание услуг, контроль |
| Способ взаимодействия с сетью электросвязи | Проводной доступ, доступ через VPN |

4.  Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

|  |  |
| --- | --- |
| Наименование лица, эксплуатирующего объект | <Наименование МО> |
| Адрес (местонахождение) лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Адрес фактического местонахождения лица, эксплуатирующего объект | Нижегородская область, г. , ул. |
| Элемент (компонент) объекта, который эксплуатируется лицом | Все компоненты |

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

|  |  |
| --- | --- |
| Программно-аппаратные средства | пользовательские компьютеры, серверы, телекоммуникационное оборудование |
| Общесистемное программное обеспечение | Ubuntu linux, windows, ... |
| Прикладное программное обеспечение | РМИС |
| Средства защиты информации | ViPNet Client 4, сертификат 12345, ПАК Jacarta, сертификат 12345, Антивирус Kaspersky Endpoint 10, сертификат 12345 |

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

|  |  |
| --- | --- |
| Категория нарушителя | Внешний нарушитель с низким потенциалом |
| Угрозы безопасности информации | Угроза несанкционированного доступа за счет заражения вредоносным кодом  Угроза атак на уровне сети  Угроза удаленного подбора пароля |

7.  Возможные последствия в случае возникновения компьютерных инцидентов

|  |  |
| --- | --- |
| Типы компьютерных инцидентов | отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта |
| Возможные последствия от компьютерных инцидентов | причинение ущерба жизни и здоровью людей отсутствует |

8.  Категория значимости, которая присвоена объекту критической информационной инфраструктуры

|  |  |
| --- | --- |
| Категория значимости объекта | Без категории |
| Результаты оценки показателей | причинение ущерба жизни и здоровью людей отсутствует |

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

|  |  |
| --- | --- |
| Организационные меры | установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта |
| Технические меры | идентификация и аутентификация, управление доступом, ограничение программной среды, антивирусная защита, межсетевое экранирование, VPN |

|  |  |  |
| --- | --- | --- |
| <Руководитель МО> | <Подпись> | <ФИО> |
| <Наименование МО> |  |  |