Дорожная карта

выполнения положений 187-ФЗ и требований 127-ПП

в государственных медицинских организациях Ростовской области

I. Принятые сокращения

187-ФЗ – Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

127-ПП – Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры РФ, а также Перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значение».

Рекомендации – Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения, утвержденные заместителем Министра здравоохранения Российской Федерации 05.04.2021 года (режим доступа – официальный сайт ГБУ РО «МИАЦ» – https://miacrost.ru, раздел «Руководителям здравоохранения», подраздел «Нормативные документы».

КИИ – критическая информационная инфраструктура.

ИС – информационная система.

ИТКС – информационно-телекоммуникационная сеть.

АСУ – автоматизированная система управления.

Перечень – перечень объектов критической информационной инфраструктуры.

Категорирование – процедура анализа критичности объекта КИИ в соответствии с «Перечнем показателей критериев значимости объектов критической информационной инфраструктуры РФ», утвержденных Постановлением Правительства РФ от 08.02.2018 № 127 и присвоение

объекту КИИ одной из категорий значимости, либо установление отсутствия необходимости присвоения ему одной из таких категорий.

Сведения – сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо отсутствии необходимости присвоения ему одной из таких категорий.

ФСТЭК – Управление Федеральной службы по техническому и экспортному контролю России по Южному и Северо-Кавказскому федеральным округам по , адрес: 344079, г. Ростов-на-Дону, ул. Ярослава Галана, д. 1Е/25, руководитель Управления – Камынин Константин Владимирович, справочная информация – начальник 1 отдела (по КИИ) Управления ФСТЭК по ЮФО и СКФО Чернов Николай Иванович, тел. 8(863)200-75-25; эксперт отдела Никитин Денис Геннадьевич, тел. 8(863)200-75-36, доб. 282; эксперт отдела Цыбенко Станислав Александрович, тел. 8(863)200-75-36, доб. 281, эксперт отдела Ильинов Денис Александрович, тел. 8(863)200-75-36, доб. 246.

ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Реестр – федеральный реестр значимых объектов критической информационной инфраструктуры Российской Федерации.

ГБУ РО «МИАЦ» – государственное бюджетное учреждение Ростовской области «Медицинский информационно-аналитический центр», адрес: 344029, г. Ростов-на-Дону, проспект Сельмаш, д. 14, начальник ГБУ РО «МИАЦ» – Жиляков Сергей Александрович, справочная информация – начальник отдела защиты информации ГБУ РО «МИАЦ» Шарыгин Алексей Валерьевич, тел. 8(863)201-70-25, 8(863)200-18-29, 8(863)201-72-39 или в закрытой группе мессенджера Telegram, (режим доступа – https://t.me/+amTO6cSsohIzM2Ji).

II. Основные термины и определения, установленные федеральным законодательством

1. Сфера здравоохранения, в полном объеме, включена в состав критической информационной инфраструктуры Российской Федерации.

Вывод: все государственные организации, входящие в сферу здравоохранения являются частью критической информационной инфраструктуры Российской Федерации.

2. Субъекты КИИ – государственные медицинские организации, которым принадлежат объекты КИИ, функционирующие в сфере здравоохранения. Объекты КИИ – это ИС, ИТКС, АСУ.

Вывод: любая медицинская организация, использующая в своей деятельности компьютерную технику имеет объекты КИИ.

3. Информационная система (ИС) – технологическая совокупность баз данных, содержащих медицинскую информацию и (или) персональные данные, программ и технических средств (ПЭВМ) для их обработки, даже если информационная система образована одним ПЭВМ с одной базой данных.

Вывод: все нематериальные активы, проходящие по бухгалтерскому учету и принадлежащие организации на праве собственности, подходящие под данное определение являются информационными системами.

4. Информационно-телекоммуникационная сеть (ИТКС) – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием ПЭВМ.

Вывод: два и более персональных компьютеров, объединенных между собой сетевым оборудованием и способных вести обмен файлами и сообщениями являются информационно-телекоммуникационной сетью.

5. Автоматизированная система управления (АСУ) – комплекс, состоящий из медицинского оборудования, управляющей им программы, установленной на ПЭВМ и предназначенный для управления различными процессами в сфере оказания медицинских услуг организации.

Вывод: сложное медицинское оборудование (УЗИ-аппараты, рентгеновские аппараты, флюорографы и рентген-установки, КТ, МРТ, лазерное оборудование (медицинское и косметическое), эндоскопическое оборудование), управляемое медицинским персоналом с помощью специальной программы, установленной на ПЭВМ – автоматизированная система управления.

III. Порядок проведения категорирования объектов КИИ:

1. Создание постоянно действующей комиссии по категорированию объектов КИИ, установление ей обязанностей и полномочий (приложение Рекомендаций, стр. 92-101).

2. Определение бизнес-процессов в деятельности каждой медицинской организации:

- составление Реестра всех управленческих, технологических, производственных, финансово-экономических и (или) иных бизнес-процессов и оценка их критичности (приложение № 7 Рекомендаций, стр. 106-116);

- формирование Перечня критических бизнес-процессов (приложение № 9 Рекомендаций, стр. 122-123).

3. Инвентаризация (ревизия) ИС, ИТКС, АСУ и их отнесение к объектам КИИ в каждой медицинской организации (в том числе и в подведомственных территориально выделенных структурных подразделениях, не имеющих статус юридического лица).

4. Составление Перечня объектов КИИ (с обязательным внесением в наименование объекта его полного названия согласно сертификата на эксплуатацию или данных (материальных или нематериальных активов) бухгалтерского учета организации), оформление Перечня в строгом соответствии с образцом (приложение № 12 Рекомендаций, стр. 127), его *обязательная* подпись всеми членами комиссии.

5. Утверждение Перечня руководителем организации (рекомендуется не *проставлять дату* утверждения документа во избежание превышения максимального срока доставки Перечня во ФСТЭК (не более 10 суток) из-за неизвестного срока согласования Перечня с учредителем).

6. *Согласование* второго экземпляра Перечня с министром здравоохранения Ростовской области.

7. Направление согласованного Перечня (после постановки даты утверждения документа) в *десятидневный срок* во ФСТЭК с обязательным сопроводительным письмом по установленному образцу (приложение № 17 Рекомендаций, стр. 145). Направлять на имя руководителя Управления ФСТЭК – Камынина Константина Владимировича. Способ отправки – заказным письмом с уведомлением о вручении Почтой России с приложением электронной копии в формате *.ods (*.odt), записанной на компакт-диск. Отправляемой корреспонденции присваивать ограничительную пометку – «Для служебного пользования» с соблюдением правил и порядка обращения с документами ограниченного доступа и приложением двух реестров с печатью организации-отправителя. Допускается передача указанного пакета документов нарочным (представителем организации).

8. Категорирование каждого объекта КИИ (согласно утвержденного Перечня) постоянно действующей комиссией (п. 1 Дорожной карты) с составлением Акта (приложение № 16 Рекомендаций, стр. 143-144).

9. Занесение результатов категорирования в Сведения, оформленные в строгом соответствии с формой, установленной приказом ФСТЭК России от 22.12.2017 № 236 (приложение № 17 Рекомендаций, стр. 147-152).

10. Представление Сведений во ФСТЭК в *десятидневный срок* после утверждения Акта категорирования (п. 8 Дорожной карты) с обязательным сопроводительным письмом по установленному образцу (приложение № 17 Рекомендаций, стр. 146). Направлять на имя руководителя Управления ФСТЭК – Камынина Константина Владимировича. Способ отправки – заказным письмом с уведомлением о вручении Почтой России с приложением электронной копии в формате *.ods (*.odt), записанной на компакт-диск. Отправляемой корреспонденции присваивать ограничительную пометку – «Для служебного пользования»

с соблюдением правил и порядка обращения с документами ограниченного доступа и приложением двух реестров с печатью организации-отправителя. Допускается передача указанного пакета документов нарочным.

10.1. Акт категорирования, его копию и копии других документов во ФСТЭК, а также своему учредителю для согласования *не направлять*. Данные документы являются внутренними и представляются только регуляторам в ходе выездных проверок.

11. Получение заключений от ФСТЭК о направлении ваших Сведений в ГосСОПКА (объекты без категории) или в Реестр (объекты с категорией значимости).

11.1. В случае несогласия регулятора с решением постоянно действующей комиссии медицинской организации о признании объектов КИИ значимыми (не значимыми) или неправильным оформлением документов – *устранение* указанных недостатков в *десятидневный срок*.

12. По мере выполнения мероприятий по категорированию объектов КИИ вносить соответствующие данные в Таблицу 3001 «Критическая информационная инфраструктура (КИИ)» в разделе «ИТ-Мониторинг» информационной системы «ИАС ГБУ РО «МИАЦ» «БАРС. Мониторинг - Здравоохранение»,а именно:

– номер и дата Приказа о создании комиссии по категорированию объектов КИИ;

– общее количество объектов КИИ;

– дата утверждения Перечня объектов КИИ;

– дата, фамилия, инициалы и должность с кем произведено согласование Перечня;

– исходящий номер и дата, отправленного во ФСТЭК Перечня объектов КИИ;

– исходящий номер и дата отправленных во ФСТЭК Сведений о результатах присвоения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;

– заключение от ФСТЭК.

13. После получения официального ответа от ФСТЭК о направлении ваших Сведений в ГосСОПКА (объекты без категории) или в Реестр (объекты с категорией значимости) внести в Модальную Таблицу 3001 информационной системы «ИАС ГБУ РО «МИАЦ» «БАРС. Мониторинг - Здравоохранение» только *значимые объекты КИИ за медицинскую организацию.*

14. Доклад непосредственного исполнителя Дорожной карты своему руководителю медицинской организации о выполнении 1 этапа создания системы безопасности критической информационной инфраструктуры этой медицинской организации.

15. В случае проведения категорирования в 2019-2022 годах и отправки Сведений в Центральный аппарат ФСТЭК (г. Москва), а также в связи с реорганизацией (сменой юридического названия организации) медицинским организациям Ростовской области требуется провести процедуру категорирования объектов КИИ ПОВТОРНО.