"УТВЕРЖДАЮ"
Начальник КГБУЗ ККМИАЦ
_____ Евминенко С.А.
"30" ноября 2018 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по категорированию объектов критической информационной инфраструктуры в медицинских организациях Красноярского края

Красноярск, 2018

Список исполнителей

СОГЛАСОВАНО:

Заместитель начальника по информационным технологиям КГБУЗ ККМИАЦ	30.11.2018 подпись, дата	Никитина М.И.
главный внештатный специалист министерства здравоохранения Красноярского края по информационной безопасности	30.11.18 подпись, дата	Демин С.Л.

ИСПОЛНИТЕЛИ:

начальник отдела информационной безопасности КГБУЗ ККМИАЦ	28.11.2018 подпись, дата	Потылицын А.Н.
Специалист по защите информации отдела информационной безопасности КГБУЗ ККМИАЦ	Зернова 28.11.2018 подпись, дата	Зернова Д.Ф.

I. Общие положения

1. Настоящие Методические рекомендации разработаны для медицинских организаций Красноярского края с целью разъяснения порядка категорирования объектов критической информационной инфраструктуры (далее – КИИ) в сфере здравоохранения.

2. Правовой основой Методических рекомендаций являются:

федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

постановление Правительства РФ от 08.02.2018 N 127 «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»;

приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

приказ ФСТЭК России от 22.12.2017 N 236 «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»;

приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

приказ ФСТЭК России от 06.12.2017 N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;

информационное сообщение ФСТЭК России от 24 августа 2018 г. N 240/25/3752 по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

3. Организационные меры, приведенные в настоящих Методических рекомендациях, могут быть расширены с учетом положений нормативно-правовых актов, указанных в п. 2.

4. В Методических рекомендациях используются следующие термины и определения:

значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры,

сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

критическая информационная инфраструктура (КИИ) – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

объекты критической информационной инфраструктуры (объекты КИИ) – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

реестр значимых объектов критической информационной инфраструктуры – реестр, который формируется и ведется ФСТЭК России на основе сведений, предоставляемых субъектами КИИ, в целях учета значимых объектов критической информационной инфраструктуры;

субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, 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, 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.

II. Создание комиссии по категорированию

5. Для проведения категорирования объектов КИИ решением руководителя медицинской организации (МО) создается комиссия по категорированию. Форма приказа приведена в Приложении 1.

6. Комиссия по категорированию состоит из следующих сотрудников:

руководитель МО или уполномоченное им лицо;

специалисты в области осуществляемых видов деятельности согласно устава, лицензии;

специалисты в области информационных технологий и связи;

специалисты по эксплуатации медицинского оборудования, учету опасных веществ и материалов;

работники, уполномоченные в области безопасности (информационной безопасности) объектов КИИ в МО;

работники, уполномоченные в области ГО и ЧС.

7. Комиссия по категорированию выполняет следующие действия:

определение процессов в рамках осуществления видов деятельности МО (субъекта КИИ);

выявление критических процессов;

выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации;

анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;

оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;

установление каждому из объектов КИИ одой из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости с последующим оформлением соответствующего акта.

III. Формирование перечня объектов КИИ

8. Категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические или иные процессы в рамках осуществления видов деятельности МО (субъекта КИИ).

9. Для определения процессов, указанных в п. 8, рекомендуется опираться на виды деятельности МО, закрепленные в уставе МО и в лицензии на осуществление медицинской деятельности.

10. Перечень типовых видов деятельности и обеспечивающих их процессов приведен в Приложении 2 к настоящим Методическим рекомендациям. Данный перечень может быть изменен с учетом специфики работы МО.

11. После составления перечня процессов необходимо для каждого из них определить, является ли он критическим, то есть процессом, нарушение и (или) прекращение которого может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

12. При определении критичности процесса рекомендуется пользоваться перечнем показателей критериев значимости (утвержден постановлением Правительства от 08.02.2018 N 127). Для сферы здравоохранения характерны показатели, относящиеся к типу «социальная значимость»:

причинение ущерба жизни и здоровью людей;

отсутствие доступа к государственной услуге, оцениваемое в максимально допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги.

13. По результатам выявления критических процессов определяются объекты 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. Формируется перечень объектов КИИ, подлежащих категорированию.

14. Перечень объектов КИИ подлежит согласованию с министерством здравоохранения Красноярского края. Для согласования в министерство здравоохранения Красноярского края направляются следующие документы:

перечень объектов КИИ, составленный по форме, рекомендованной информационным сообщением ФСТЭК России от 24 августа 2018 г. N 240/25/3752 по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Форма приведена в Приложении 3;

пояснительная записка по форме, приведенной в Приложении 4, содержащая информацию о видах деятельности МО, обеспечивающих их процессах, критических процессах, объектах КИИ.

15. После согласования с министерством здравоохранения Красноярского края перечень объектов КИИ утверждается руководителем МО. В течение 5 рабочих дней после утверждения перечень объектов КИИ направляется во ФСТЭК России (105066, г. Москва, ул. Старая Басманная, д. 17), копия направляется во ФСТЭК России по Сибирскому федеральному округу (630091, г. Новосибирск, Красный проспект, д. 41). При направлении сведений следует приложить электронную копию перечня объектов КИИ на компакт-диске в формате редактируемого офисного документа.

16. В случае отсутствия в МО объектов КИИ в министерство здравоохранения Красноярского края направляется пояснительная записка по форме, приведенной в Приложении 4. Предоставление информации об отсутствии в организации объектов КИИ во ФСТЭК России в соответствии с законодательством о безопасности критической информационной инфраструктуры Российской Федерации не требуется.

IV. Категорирование объектов КИИ

17. В соответствии с перечнем показателей критериев значимости (утвержден постановлением Правительства от 08.02.2018 N 127) каждому объекту КИИ присваивается одна из категорий значимости либо принимается решение об отсутствии необходимости присвоения одной из категорий. Данное решение принимается комиссией по категорированию исходя из

оценки масштабов возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.

18. Показатели критериев значимости подразделяются на пять типов:

социальная значимость;

политическая значимость;

экономическая значимость;

экологическая значимость;

значимость для обеспечения обороны страны, безопасности государства и правопорядка.

19. Для сферы здравоохранения характерны показатели, относящиеся к типу «социальная значимость»:

причинение ущерба жизни и здоровью людей;

отсутствие доступа к государственной услуге, оцениваемое в максимально допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги.

20. Максимальный срок категорирования не должен превышать одного года со дня утверждения МО (субъектом КИИ) перечня объектов.

21. Решение комиссии о присвоении категории каждому объекту КИИ оформляется актом. Акт утверждается руководителем МО и хранится до вывода объекта КИИ из эксплуатации.

22. Акт должен содержать следующие сведения:

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;

сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями ФСТЭК России (приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

23. Форма акта приведена в Приложении 5 к настоящим Методическим рекомендациям.

V. Направление сведений о категорировании во ФСТЭК России

24. В течение 10 дней со дня утверждения акта, указанного в п. 20, необходимо направить во ФСТЭК России сведения о каждом объекте КИИ из утвержденного перечня (п. 15):

сведения об объекте КИИ;

сведения о субъекте КИИ;

сведения о взаимодействии объекта КИИ и сетей электросвязи;

сведения о лице, эксплуатирующем объект КИИ;

сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ, в том числе средствах, используемых для обеспечения безопасности объекта КИИ и их сертификатах соответствия требованиям по безопасности информации (при наличии);

сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта КИИ либо об отсутствии таких угроз;

возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ либо сведения об отсутствии таких последствий;

категорию значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;

организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ, либо сведения об отсутствии необходимости применения указанных мер.

25. Форма направления сведений, указанных в п. 24, утверждена приказом ФСТЭК России от 22.12.2017 N 236 и приведена в Приложении 6 к настоящим Методическим рекомендациям. Сведения направляются во ФСТЭК России (105066, г. Москва, ул. Старая Басманная, д. 17), копия направляется во ФСТЭК России по Сибирскому федеральному округу (630091, г. Новосибирск, Красный проспект, д. 41). При направлении сведений следует приложить электронную копию сведений на компакт-диске в формате редактируемого офисного документа.

26. ФСТЭК России в тридцатидневный срок со дня получения вышеуказанных сведений проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту КИИ одной из категорий значимости либо неприсвоения ему ни одной из таких категорий и в зависимости от правильности проведенного категорирования:

вносит в реестр сведения об объекте КИИ в реестр значимых объектов КИИ, о чем в десятидневный срок уведомляет субъекта КИИ;

отказывает во внесении в реестр в десятидневный срок с мотивированным обоснованием причин отказа.

27. В случае получения мотивированного обоснования причин отказа субъект КИИ не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения по указанной форме во ФСТЭК России.

VI. Изменение установленной категории значимости

28. Категория значимости объекта КИИ подлежит изменению в следующих случаях:

по мотивированному решению ФСТЭК России, принятому по результатам проверки;

в случае изменения объекта КИИ, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений,

на основании которых ему была присвоена определенная категория значимости;

в связи с ликвидацией, реорганизацией субъекта КИИ и (или) изменением его организационно-правовой формы.

29. Пересмотр установленной категории значимости осуществляется не реже чем один раз в 5 лет. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются во ФСТЭК России.

Приложение 1
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

ПРОЕКТ ПРИКАЗА

_____ № _____

_____
(наименование населенного пункта)

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», постановлением Правительства РФ от 08.02.2018 № 127 «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», в целях организации проведения работ по категорированию объектов критической информационной инфраструктуры в <полное наименование МО>:

ПРИКАЗЫВАЮ:

1. Создать комиссию по категорированию объектов критической информационной инфраструктуры (далее – КИИ).
2. Утвердить:

Состав комиссии по категорированию объектов критической информационной инфраструктуры согласно приложению № 1;

Положение о комиссии по категорированию объектов критической информационной инфраструктуры согласно приложению № 2.

3. Комиссии организовать работу по категорированию объектов КИИ <наименование МО> в сроки, предусмотренные Приказом министерства здравоохранения Красноярского края № 1286-орг от 29.11.2018 г.
4. Контроль за исполнением настоящего приказа оставляю за собой.

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Приложение № 1
к приказу <наименование МО>
от «__»_____ г. № _____

Состав комиссии <наименование МО> объектов
критической информационной инфраструктуры

_____ – _____,
(ФИО) (должность)

председатель комиссии

_____ – _____,
(ФИО) (должность)

заместитель председателя комиссии

Члены комиссии:

_____ – _____
(ФИО) (должность)

_____ – _____
(ФИО) (должность)

_____ – _____
(ФИО) (должность)

_____ – _____
(ФИО) (должность)

Приложение № 2
к приказу <наименование МО>
от «__»_____ г. № _____

Положение
о комиссии по категорированию объектов
критической информационной инфраструктуры

1. Общие положения

1.1. Настоящее Положение о комиссии по категорированию объектов критической информационной инфраструктуры (далее - Положение), определяет функции, порядок и обеспечение деятельности комиссии по категорированию объектов критической информационной инфраструктуры (далее - Комиссия).

1.2. Комиссия создается для организации работ по категорированию объектов критической информационной инфраструктуры в <наименование МО>.

1.3. Комиссия является постоянно действующим консультативно-совещательным органом <наименование МО>.

1.4. Комиссия руководствуется в своей деятельности правовыми актами Российской Федерации, Красноярского края и настоящим Положением.

2. Функции комиссии

2.1. Функциями Комиссии являются:

а) определение процессов, в рамках выполнения функций (полномочий) или осуществления видов деятельности <наименование МО>, как субъекта критической информационной инфраструктуры;

б) выявление наличия критических процессов в <наименование МО>;

в) выявление объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, подготовка предложений для включения в перечень объектов;

г) рассмотрение возможных действий нарушителей в отношении объектов критической информационной инфраструктуры, а также иных источников угроз безопасности информации;

д) анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах

критической информационной инфраструктуры;

е) оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

ж) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости.

3. Порядок и обеспечение деятельности комиссии

3.1. Заседания Комиссии проводятся по мере необходимости по решению председателя Комиссии.

3.2. Заседание Комиссии считается правомочным при присутствии на нем не менее половины от общего числа членов Комиссии.

Присутствие на заседании Комиссии иных лиц, кроме членов Комиссии, допускается с разрешения председателя Комиссии.

3.3. Председатель Комиссии:

назначает дату, время и место проведения заседаний Комиссии;

утверждает повестку заседания Комиссии;

руководит заседанием Комиссии;

распределяет обязанности между членами Комиссии;

подписывает заключения и иные документы, подготовленные Комиссией;

пользуется правами члена Комиссии наравне с другими членами Комиссии.

В случае отсутствия председателя Комиссии его полномочия осуществляет заместитель председателя Комиссии.

3.4. Секретарь Комиссии:

координирует деятельность членов Комиссии;

готовит проекты повесток заседаний Комиссии и представляет на утверждение председателю Комиссии;

своевременно информирует членов Комиссии о дате, времени, месте и повестке заседаний Комиссии;

в случае необходимости совместно с членами Комиссии готовит информацию, документы, иные материалы к заседаниям Комиссии;

в течение 3 рабочих дней с даты проведения заседания Комиссии и в соответствии с ее решением готовит заключение и представляет его на подпись председателю Комиссии, заместителю председателя Комиссии, иным членам Комиссии;

организует и ведет делопроизводство Комиссии.

3.5. Члены Комиссии имеют право:

участвовать в работе Комиссии;

участвовать в обсуждении вопросов, включенных в повестку заседания Комиссии, вносить по ним предложения;

знакомиться с информацией, документами и материалами по вопросам, вынесенным на обсуждение Комиссии, на стадии их подготовки, вносить свои предложения;

в случае несогласия с принятым решением изложить свое особое мнение в письменном виде, которое прилагается к соответствующему заключению Комиссии.

3.6. Решения Комиссии принимаются простым большинством голосов членов Комиссии как присутствующих на заседании, так и отсутствующих, выразивших свое мнение в письменном виде и представивших его на заседание Комиссии.

Каждый член Комиссии имеет один голос. При равенстве голосов принятым считается решение, за которое проголосовал председательствующий на заседании Комиссии.

По итогам работы Комиссии оформляется акт, который содержит сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры 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 критической информационной инфраструктуры, установленными ФСТЭК России.

Акт подписывается председателем, заместителем председателя, секретарем и другими членами Комиссии и утверждается <руководитель МО>.

3.8. Организационное и материально-техническое обеспечение деятельности Комиссии осуществляет <наименование МО>.

Приложение 2
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

Перечень типовых видов деятельности в сфере здравоохранения и обеспечивающих их процессов

Вид деятельности	Все процессы в рамках осуществления вида деятельности
Оказание медицинской помощи	**Амбулаторно-поликлиническая помощь**
	Прием заявок на оказание медицинской помощи
	Регистрация пациента
	Осмотр пациента
	Организация сестринского дела
	Лекарственное обеспечение, лекарственная терапия
	Оперативное вмешательство
	Оказание скорой и неотложной медицинской помощи
	Реанимационные мероприятия
	Направление на МСЭ
	Направление на госпитализацию
	Экспертиза временной нетрудоспособности
	Экспертиза качества
	Иные процессы в МО
	...
	Стационар
	Прием заявок на оказание медицинской помощи
	Регистрация пациента
	Осмотр пациента
	Организация сестринского дела
	Лекарственное обеспечение, лекарственная терапия
	Оперативное вмешательство
	Оказание скорой и неотложной медицинской помощи
	Реанимационные мероприятия
	Направление на МСЭ
	Экспертиза временной нетрудоспособности
	Выписка
	Иные процессы в МО
	...

Оказание медицинской помощи	**Параклиническая диагностика**
	Рентгенологические исследования
	Функциональная диагностика
	Ультразвуковая диагностика
	Эндоскопические исследования
	Лучевая диагностика
	Клинико-лабораторная диагностика
	Иные процессы в МО
	...
	Профилактика и восстановление
	Диспансеризация взрослого населения, профилактические осмотры, Диспансеризация раз в 2-года
	Диспансерное наблюдение отдельных груп населения
	Физиотерапия, ЛФК, медицинский массаж
	Иные процессы в МО
	...
	Организация высокотехнологичной медицинской помощи
	Регистрация случаев необходимости оказания ВМП
	Направление на ВМП
	Оказание ВМП
	Иные процессы в МО
	...
Работы (услуги) по транспортировке и хранению донорской крови и(или) ее компонентов	Транспортировка и хранение донорской крови и(или) ее компонентов
	Переливание крови
Донорство органов	Медицинское обследование донора
	Изъятие, хранение, транспортировка донорских органов
	Трансплантация донорских органов
Патологоанатомическая деятельность	Проведение патологоанатомических исследований
Деятельность по эксплуатации комплекса, в котором содержатся радиоактивные вещества	Эксплуатация комплекса, в котором содержатся радиоактивные вещества
Деятельность по обороту наркотических средств, психотропных веществ и их прекурсоров, культивированию наркосодержащих растений	Оборот наркотических средств, психотропных веществ и их прекурсоров,
Деятельность по сбору, обеззараживанию, временному хранению и транспортировке опасных отходов	Сбор, обеззараживание, временное хранению и транспортировка опасных отходов

Деятельность, связанная с использованием возбудителей инфекционных заболеваний	Вакцинация
Проведение клинических исследований лекарственных препаратов для медицинского применения	Клинические исследования лекарственных препаратов для медицинского применения
Организация лечебного питания	Организация лечебного питания
Организация медицинского документооборота	Внутренний и внешний медицинский документооборот
	Хранение электронных медицинских документов
	Формирование, хранение и проверка электронных подписей
Медицинская статистика	Сбор, свод, хранение показателей
	Статистический анализ показателей, формирование отчетов
Обеспечение информационных технологий	Обеспечение функционирования информационной инфраструктуры, в том числе критической
	Защита объектов критической информационной инфраструктуры, ИСПДн и ГИС
Административно-хозяйственная деятельность, направленная на обеспечение деятельности Учреждения	Бухгалтерский учет
	Кадровый учет
	Формирование отчетности о хозяйственной деятельности
	Внутренний и внешний документооборот
	Формирование, хранение и проверка электронных подписей
Медико-санитарное просвещение, проведение семинаров, лекций, иных мероприятий	Организация работы Школы здоровья, Центра Здоровья и др.
Аренда помещений	Сдача имущества в аренду
Услуги по организации общественного питания	Организация общественного питания
Предоставление одноместной или двухместной палат	Предоставление палат
иные виды деятельности МО	иные процессы МО

Приложение 3
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ
<руководитель МО>

_____

«_____»_____ 20___ г.

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[2]
			Здравоохранение		
			Здравоохранение		
			Здравоохранение		

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Приложение 4
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

УТВЕРЖДАЮ
<руководитель МО>

_____

«_____»_____ 20___ г.

Пояснительная записка по процессам осуществления видов деятельности и критическим процессам

Вид деятельности	Все процессы в рамках осуществления вида деятельности	Отметка о критичности процесса (да/нет)	ИС; АСУ; сети, обеспечивающие функционирование критических процессов

Приложение 5
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

УТВЕРЖДАЮ
<руководитель МО>

_____

«_____»_____ 20___ г.

Форма типового Акта
категорирования объекта критической информационной инфраструктуры

_____
(наименование объекта)

На основании приказа от «___» _____ 20__ г. №_____ комиссия в составе:

председатель комиссии: _____
(должность, фамилия, инициалы)

члены комиссии: _____
(должность, фамилия, инициалы)

_____
(должность, фамилия, инициалы)

_____
(должность, фамилия, инициалы)

В соответствии с требованиями федерального закона от 26.07.2017 г. № 187-ФЗ, постановления Правительства РФ от 08.02.2018 г. № 127 провела категорирование объекта критической информационной инфраструктуры _____
(наименование объекта)

В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее - КИИ).
2. Сведения об угрозах безопасности информации объекта КИИ.
3. Реализованные на объекте КИИ меры по обеспечению безопасности.
4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости.

Вышеуказанные сведения представлены в Приложении 1 к настоящему Акту.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018 г. № 127 объекту _____
(наименование объекта)

присвоена категория _____.

Состав необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, утвержденными приказом ФСТЭК России от 25.12.2017 № 239, представлен в Приложении 2.

Председатель комиссии: _____/_____

Члены комиссии: _____/_____
_____/_____
_____/_____

Приложение 1

Сведения об объекте КИИ:

Наименование объекта	
Адреса размещения объекта	
Сфера (область) деятельности, в которой функционирует объект	
Назначение объекта	
Критические процессы, которые обеспечиваются объектом	
Архитектура объекта	

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ:

Программно-аппаратные средства	Пользовательские компьютеры - шт. Серверы - шт. Телекоммуникационное оборудование - шт. Средства беспроводного доступа - шт. Производственное оборудование - шт. Иные программно-аппаратные средства - шт.
Общесистемное программное обеспечение	Наименования операционных систем: Средства виртуализации:
Прикладное программное обеспечение	
Средства защиты информации	

Сведения о взаимодействии объекта КИИ и сетей электросвязи:

Категория сети электросвязи	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи	
Способ взаимодействия с сетью электросвязи	

Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ:

Категория нарушителя	
Угрозы безопасности информации	

Возможные последствия в случае возникновения компьютерных инцидентов:

Типы компьютерных инцидентов	
Возможные последствия от компьютерных инцидентов	

Реализованные организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ:

Организационные меры	
Технические меры	

Перечень показателей критериев значимости и их значения:

№	Показатель	Значение показателя	Категория
	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, для которых могут быть недоступны транспортные услуги (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)		
	Политическая значимость		
6	Прекращение или нарушение функционирования государственного органа в части невыполнения		

№	Показатель	Значение показателя	Категория
	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		
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		

№	Показатель	Значение показателя	Категория
	значений)		
	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)		
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)		

Приложение 2

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости:

Обозначение меры	**Меры обеспечения безопасности значимого объекта**

Приложение 6
к Методическим рекомендациям по
категорированию объектов критической
информационной инфраструктуры в
медицинских организациях Красноярского края

Форма направления Сведений 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	
1.2	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	
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»	
1.4	Назначение объекта	
1.5	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	
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)	

2. 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) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	

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	
3.2	Наименование оператора связи	
3.3	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	

4. 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)	

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, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	
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)	
5.4	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации	

	(идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации	

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	
6.2	Основные угрозы безопасности информации или обоснование их неактуальности	

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	
7.2	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» или обоснование отсутствия возможности причинения ущерба вследствие	

	компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1	Категория значимости, которая присвоена объекту	
8.2	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	

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)	
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	

_____	_____	_____
(должность руководителя МО)	(подпись)	(инициалы, фамилия)

М.П.

«___» _____ 20___ г.