ПРОЕКТ

Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения

на ___ листах

г. Москва, 2020

Оглавление

1. ВВЕДЕНИЕ

1. Все организации, осуществляющие деятельность в сфере охраны здоровья (далее – организации сферы здравоохранения), которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, являются субъектами критической инфраструктуры.

Для целей категорирования объектов критической информационной инфраструктуры под «иным законным основанием» понимается передача прав пользования информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления на основании правовых актов или решений собственника без передачи права собственности на них. Например, на основании договора безвозмездного пользования[1], договора на право хозяйственного ведения[2], договора на право оперативного управления[3].

В соответствии с требованиями законодательства Российской Федерации, организации сферы здравоохранения как субъекты критической инфраструктуры должны установить соответствие принадлежащих им объектов критической информационной инфраструктуры критериям значимости и показателям их значений.

2. Настоящие методические рекомендации содержат рекомендации по отнесению информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления организаций сферы здравоохранения к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры с последующим установлением одной из

[1] ГК РФ, ст. 689
[2] ГК РФ, ст. 294
[3] ГК РФ, ст. 296

категорий значимости объектов критической информационной инфраструктуры либо принятием решения об отсутствии оснований для их отнесения к значимым объектам критической информационной инфраструктуры.

3. Настоящие методические рекомендации описывают и детализируют типовую процедуру категорирования объектов критической информационной инфраструктуры организаций сферы здравоохранения в соответствии с критериями, установленными постановлением Правительства Российской Федерации от 08.02.2018 № 127, применительно к организациям сферы здравоохранения.

Перечень основных нормативных правовых актов, использованных при разработке настоящих методических рекомендаций, приведен в Приложении 2.

Перечень организаций сферы здравоохранения, на которые распространяется область действия настоящих методических рекомендаций, приведен в Приложении 3.

Примеры информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере здравоохранения, приведены в Приложении 4.

4. Настоящие методические рекомендации применяются субъектами критической информационной инфраструктуры для:

– определения состава бизнес-процессов[4] в рамках видов деятельности организации сферы здравоохранения и выявления критичных управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов организации сферы здравоохранения, нарушение или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим

[4] В настоящих методических рекомендациях применяется термин «бизнес-процесс», аналогичный определению «процесс» из постановления Правительства Российской Федерации от 08.02.2018 г. № 127

последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка;

– определения информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей, которые обрабатывают информацию, необходимую для обеспечения критичных процессов, или осуществляют управление, контроль или мониторинг критичных процессов организации сферы здравоохранения;

– формирования перечня объектов критической информационной инфраструктуры организации сферы здравоохранения, подлежащих категорированию;

– оценки для каждого объекта критической информационной инфраструктуры организации сферы здравоохранения масштаба возможных последствий в случае возникновения компьютерных инцидентов;

– присвоения каждому из объектов критической информационной инфраструктуры организации сферы здравоохранения одной из категорий значимости либо принятия решения об отсутствии необходимости присвоения ему одной из категорий значимости;

– подготовки сведений о результатах присвоения объекту критической информационной инфраструктуры организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России).

5. Настоящие методические рекомендации носят рекомендательный характер и применяются наряду с методическими документами, определяющими порядок категорирования объектов критической информационной инфраструктуры, разработанными органом

исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России), а также исполнительными органами государственной власти субъектов Российской Федерации в сфере охраны здоровья.

6. Для целей настоящих методических рекомендаций используются термины и определения, установленные законодательством Российской Федерации о безопасности критической информационной инфраструктуры и национальными стандартами в области защиты информации. Основные термины, определения и сокращения, используемые в настоящих методических рекомендациях, приведены в Приложении 1.

7. Категорирование объектов критической информационной инфраструктуры осуществляется постоянно действующей комиссией по категорированию, создаваемой в организации сферы здравоохранения. При создании постоянно действующей комиссии по категорированию и определении порядка направления в ФСТЭК России сведений необходимо руководствоваться пунктами 11 – 13, 15 – 18 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 № 127.

Рекомендации по формированию постоянно действующей комиссии по категорированию объектов критической инфраструктуры организации сферы здравоохранения приведены в Приложении 5.

2. ОПИСАНИЕ ПРОЦЕДУРЫ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КИИ

2.1. Общие положения

8. Процедура категорирования объектов критической информационной инфраструктуры осуществляется на основании и в соответствии с

федеральным законом[5], а также Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации[6] и Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными постановлением Правительства Российской Федерации от 08.02.2018 № 127.

9. Категорированию подлежат ИС, ИТКС, АСУ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные критичные бизнес-процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности организации сферы здравоохранения.

10. В ходе процедуры категорирования ИС, ИТКС, АСУ необходимо проанализировать и оценить критичность всех возможных бизнес-процессов, реализуемых организацией сферы здравоохранения.

11. Принятие решения об отсутствии необходимости присвоения категории какой-либо ИС, ИТКС, АСУ организации сферы здравоохранения должно быть основано на результатах оценки их влияния на нарушение или прекращение критичного бизнес-процесса, приводящее к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка в соответствии с настоящими методическими рекомендациями.

Если ИС, ИТКС, АСУ организации сферы здравоохранения отнесены к объектам КИИ, но не соответствуют критериям значимости, показателям этих критериев и их значениям, таким ИС, ИТКС, АСУ не присваивается ни одна из категорий.

---

[5] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ, ст. 7

[6] Постановление Правительства Российской Федерации от 08.02.2018 № 127

12. Процедура категорирования ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения, включает следующие процессы:

– определение управленческих, технологических, производственных, финансово-экономических и (или) иных бизнес-процессов, присутствующих в организации сферы здравоохранения, и выделение из них критичных;

– определение и формирование Перечня объектов КИИ и выделение критичных объектов КИИ организации сферы здравоохранения;

– присвоение каждому объекту КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Состав процессов, осуществляемых при категорировании ИС, ИТКС, АСУ организации сферы здравоохранения, и их содержание приведены в Приложении 6.

2.2. Определение бизнес-процессов

13. Определение бизнес-процессов в деятельности организации сферы здравоохранения и выделение среди них критичных предполагает проведение анализа всех управленческих, технологических, производственных, финансово-экономических и (или) иных бизнес-процессов организации сферы здравоохранения.

14. Определение бизнес-процессов в деятельности организации сферы здравоохранения включает следующие этапы:

– составление Реестра всех управленческих, технологических, производственных, финансово-экономических и (или) иных бизнес-процессов организации сферы здравоохранения;

– высокоуровневую оценку негативных последствий от нарушения бизнес-процессов в деятельности организации сферы здравоохранения (оценка критичности бизнес-процессов);

– формирование Перечня критичных бизнес-процессов в деятельности организации сферы здравоохранения.

Этапы определения бизнес-процессов организации сферы здравоохранения и их содержание приведены в Приложении 6.

2.3. Составление Реестра бизнес-процессов

15. На этапе составления Реестра оценка критичности бизнес-процессов организации сферы здравоохранения и их влияния на возможные последствия от нарушения бизнес-процесса по критериям, определенным постановлением Правительства РФ от 08.02.2018 № 127, не проводится.

16. Для составления Реестра бизнес-процессов организации сферы здравоохранения проводится выявление и описание всех его управленческих, технологических, производственных, финансово-экономических и (или) иных бизнес-процессов.

17. На основании учредительных документов, Положения об организации сферы здравоохранения, имеющихся описаний существующих бизнес-процессов, выбранные бизнес-процессы уточняются.

При необходимости, бизнес-процессы, не характерные для данной организации сферы здравоохранения, исключаются из Реестра и добавляются специфические бизнес-процессы, выполняемые организацией сферы здравоохранения.

18. Результаты определения и описания бизнес-процессов организации сферы здравоохранения фиксируются в описательной части Реестра бизнес-процессов организации сферы здравоохранения. Форма Реестра бизнес-процессов организации сферы здравоохранения и пример ее заполнения приведены в Приложении 7.

19. Реестр бизнес-процессов подписывается Председателем постоянно действующей комиссии по категорированию и утверждается руководителем организации сферы здравоохранения.

2.4. Оценка критичности бизнес-процессов

2.4.1. Допущения и ограничения

20. При проведении высокоуровневой оценки возможных последствий от нарушения бизнес-процесса организации сферы здравоохранения не оцениваются количественные показатели критериев значимости, а дается их качественная оценка.

21. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения влияния на прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения[7], транспортной инфраструктуры[8], сетей связи[9], а также, в дальнейшем, расчет

[7] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 2, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)
[8] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 3, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

этих показателей значимости для объектов КИИ организации сферы здравоохранения не проводится, так как бизнес-процессы организаций сферы здравоохранения не задействованы:

– в управлении объектами обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, контроле или мониторинге и эксплуатации таких объектов;

– в обеспечении бесперебойного функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи;

– в поддержании качества функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи.

22. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения экономической значимости[10] проводится исключительно для организаций сферы здравоохранения, имеющих организационно-правовую форму «государственное унитарное предприятие».

23. Оценка критичности бизнес-процессов и дальнейший расчет показателей значимости для объектов КИИ с точки зрения экономической значимости[11] для организаций сферы здравоохранения иных организационно-правовых форм не проводится, так как такие организации сферы здравоохранения не являются государственными корпорациями, государственными компаниями, стратегическими акционерными обществами[12], стратегическими предприятиями[13], у которых возможно

---

[9] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 4, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

[10] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 8, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

[11] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 8, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

[12]Указ Президента РФ от 04.08.2004 № 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»

[13] Распоряжение Правительства РФ от 20.08.2009 № 1226-р «Об утверждении перечня стратегических предприятий и организаций»

снижение уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей).

24. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации[14], а также, в дальнейшем, расчет таких показателей значимости для объектов КИИ организации сферы здравоохранения, не проводится, если организация сферы здравоохранения применяет нулевую ставку по налогу на прибыль[15] и (или) оказывает медицинские услуги, освобождаемые от налогообложения[16].

25. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения влияния на прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета[17], а также, в дальнейшем, расчет таких показателей значимости для объектов КИИ организации сферы здравоохранения, не проводится, так как организации сферы здравоохранения не осуществляют для клиентов операции по банковским счетам и (или) без открытия банковского счета и не являются 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[18].

26. Оценка критичности бизнес-процессов организации сферы здравоохранения, за исключением организаций сферы здравоохранения, использующих в своей деятельности источники ионизирующего излучения, с

---

[14] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 9, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)
[15] При выполнении условий, перечисленных в ст. 284.1 НК РФ
[16] Ст. 149 НК РФ
[17] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 10, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)
[18]Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ

точки зрения экологической значимости[19], а также, в дальнейшем, расчет таких показателей значимости для объектов КИИ организации сферы здравоохранения, не проводится, так как организации сферы здравоохранения, не использующие в своей деятельности источники ионизирующего излучения, не относятся к опасным производственным объектам[20], нарушение функционирования которых может привести к авариям, инцидентам или катастрофам, влияющим на ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иных вредных воздействий[21].

27. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения значимости для обеспечения обороны страны, безопасности государства и правопорядка[22], а также, в дальнейшем, расчет таких показателей значимости для объектов КИИ организации сферы здравоохранения, не проводится, так как бизнес-процессы организации сферы здравоохранения не могут повлиять на прекращение или нарушение функционирования пункта управления (ситуационного центра) государственных органов власти или государственной корпорации, информационных систем в области обеспечения обороны страны, безопасности государства и правопорядка, снижение показателей государственного оборонного заказа.

28. Допущения и ограничения, приведенные в разделе 2.4.1 настоящих методических рекомендаций, могут быть использованы для

[19] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. 11, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

[20] Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов»

[21] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. примечание 5, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

[22] Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений. п. п. 12, 13, 14, (утв. постановлением Правительства РФ от 08.02.2018 г. № 127)

обоснования неприменимости того или иного критерия значимости для бизнес-процесса организации сферы здравоохранения.

2.4.2. Критерии оценки критичности бизнес-процессов

29. При проведении оценки необходимо учитывать, что любой бизнес-процесс организации сферы здравоохранения может быть как полностью автоматизирован, так и частично[23]. Неавтоматизированная (ручное управление) часть должна рассматриваться как составляющая оцениваемого бизнес-процесса, позволяющая исключить или снизить масштаб возможных негативных последствий, приводящих к нарушению или прекращению выполнения организацией сферы здравоохранения установленных функций (полномочий).

30. При оценке критичности бизнес-процесса с точки зрения социальной значимости оценивается влияние бизнес-процесса организации сферы здравоохранения на возможный ущерб, причиняемый жизни или здоровью людей, а также максимальное время отсутствия доступа к государственной услуге для получателей такой услуги.

31. При оценке критичности бизнес-процесса с точки зрения политической значимости оценивается влияние бизнес-процесса организации сферы здравоохранения на возможность причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики.

32. При оценке критичности бизнес-процесса с точки зрения экономической значимости оценивается влияние бизнес-процесса организации сферы здравоохранения на возможность причинения прямого и косвенного ущерба государственному унитарному предприятию.

33. Бизнес-процесс организации сферы здравоохранения считается критичным, если в ходе оценки возможных последствий от его нарушения

[23] Полностью неавтоматизированные бизнес-процессы не рассматриваются, так как они выходят из-под юрисдикции Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ст.1)

установлено, что он задействован и оказывает влияние хотя бы по одному критерию, определенному постановлением Правительства РФ от 08.02.2018 № 127.

Критерии влияния (задействованности) бизнес-процессов организации сферы здравоохранения на показатели возможных последствий приведены в разделе I Справочных материалов по оценке критичности бизнес-процессов организации сферы здравоохранения Приложения 8.

2.4.3. Порядок оценки критичности бизнес-процессов

34. На этом этапе проводится оценка возможного негативного влияния последствий от нарушения бизнес-процесса организации сферы здравоохранения по показателям, определенным постановлением Правительства РФ от 08.02.2018 № 127.

35. Используя результаты определения и описания бизнес-процессов в деятельности организации сферы здравоохранения, зафиксированные в описательной части Реестра бизнес-процессов организации сферы здравоохранения проводятся обоснование критичности бизнес-процессов организации сферы здравоохранения, проводящей категорирование объектов КИИ и оценка возможного негативного влияния последствий от нарушения бизнес-процесса. Такая оценка проводится с использованием Алгоритмов оценки значимости бизнес-процесса, приведенных в разделе II Справочных материалов по оценке критичности бизнес-процессов организации сферы здравоохранения (Приложение 8), для следующих показателей, определенных постановлением Правительства РФ от 08.02.2018 № 127:

– социальная значимость (способность причинить ущерб жизни и здоровью людей; способность привести к нарушению максимального времени отсутствия доступа в оказании государственных услуг);

– политическая значимость (способность оказывать влияние на функционирование органа государственной власти[24]);

– экономическая значимость (способность оказывать влияние на возможность причинения прямого и косвенного ущерба государственному унитарному предприятию).

При этом бизнес-процесс организации сферы здравоохранения считается способным причинить ущерб жизни и здоровью людей, если он задействован (обеспечивает) в управлении или обеспечении работоспособности механизмов и устройств, нарушение функционирования которых может привести:

– к авариям, катастрофам с человеческими жертвами;

– к бактериологическому, радиационному или химическому заражению;

– к отключению приборов, обеспечивающих жизненно важные функции организма;

– к нарушению технологий производства и хранения фармацевтической и медицинской продукции;

– к иным последствиям, пагубно влияющим на жизнь и здоровье людей.

Бизнес-процесс организации сферы здравоохранения считается способным привести к отсутствию доступа в оказании государственных услуг, если он задействован:

– в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры доступа к государственной услуге;

[24] В контексте настоящих методических рекомендаций, если это специально не оговорено, под органом государственной власти подразумеваются федеральные органы государственной власти, органы государственной власти субъекта Российской Федерации или города федерального значения

– в аналитической, экспертной, учетной деятельности, необходимой для обеспечения функционирования государственных органов власти, оказывающих государственные услуги;

– в обеспечении взаимодействия государственных органов власти, оказывающих государственные услуги.

Бизнес-процесс организации сферы здравоохранения считается оказывающим влияние на функционирование органа государственной власти, если он задействован:

– в аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений органом государственной власти;

– в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры взаимодействия органов государственной власти;

– в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры оповещения населения о чрезвычайных ситуациях;

– в поддержании бесперебойного функционирования элементов системы управления, необходимой для реализации возложенных на орган государственной власти полномочий.

Бизнес-процесс организации сферы здравоохранения считается оказывающим влияние на возможность причинения прямого и косвенного ущерба государственному унитарному предприятию, если он задействован:

– в аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений руководством государственного унитарного предприятия;

– в обеспечении взаимодействия с организациями кредитно-финансовой сферы, включая страховые компании, биржи, банки, казначейство, налоговые органы.

Для обоснования неприменимости для таких бизнес-процессов остальных показателей, определенных постановлением Правительства РФ от 08.02.2018 № 127, используется раздел «Допущения и ограничения» настоящих методических рекомендаций.

36. В случае если осуществление критичного бизнес-процесса организации сферы здравоохранения зависит от осуществления иных критичных бизнес-процессов, оценка проводится исходя из совокупного масштаба возможных последствий от нарушения или прекращения функционирования всех выполняемых критичных бизнес-процессов.

37. Результаты оценки критичности бизнес-процессов в деятельности организации сферы здравоохранения фиксируются в разделе оценки критичности Реестра бизнес-процессов организации сферы здравоохранения (Приложение 7).

2.4.4. Формирование Перечня критичных бизнес-процессов

38. После оценки критичности бизнес-процессов в деятельности организации сферы здравоохранения, из Реестра исключаются бизнес-процессы, которые не являются критичными, и формируется описательная часть Перечня критичных бизнес-процессов организации сферы здравоохранения. Форма Перечня критичных бизнес-процессов организации сферы здравоохранения представлена в Приложении 9.

2.5. Описание процесса «Определение и формирование Перечня объектов КИИ»

39. Процесс формирования Перечня объектов КИИ организации сферы здравоохранения и выделения критичных включает следующие этапы:

– ревизия и составление Перечня ИС, ИТКС, АСУ организации сферы здравоохранения;

– оценка задействованности и влияния ИС, ИТКС, АСУ в управлении, контроле и мониторинге критичных бизнес-процессов организации сферы здравоохранения;

– формирование Перечня потенциально значимых объектов КИИ организации сферы здравоохранения (Перечня объектов КИИ, подлежащих категорированию).

Состав и содержание этапов процесса формирования Перечня объектов КИИ организации сферы здравоохранения и выделения критичных приведен в Приложении 6.

2.6. Ревизия систем, имеющихся в организации сферы здравоохранения

40. В качестве источника получения сведений о наличии в организации сферы здравоохранения на праве собственности, аренды или на ином законном основании ИС, ИТКС, АСУ могут быть использованы:

– сведения из федеральной государственной информационной системы учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов[25] и аналогичных информационных систем учета субъектов Российской Федерации;

– договоры на разработку и внедрение в организации сферы здравоохранения ИС, ИТКС, АСУ;

– локальные нормативные акты организации сферы здравоохранения, определяющие порядок использования ИС, ИТКС, АСУ;

[25] Постановление Правительства РФ от 26.06.2012 № 644 «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов»

– локальные нормативные акты о вводе ИС, ИТКС, АСУ организации сферы здравоохранения в эксплуатацию;

– данные бухгалтерского учета организации сферы здравоохранения по разделу «основные средства»;

– данные бухгалтерского учета организации сферы здравоохранения по разделу «нематериальные активы»;

– проектная документация на ИС, ИТКС, АСУ организации сферы здравоохранения;

– данные управленческого учета в подразделении организации сферы здравоохранения, отвечающем за применение информационных технологий и обслуживание средств автоматизации.

41. Результаты ревизии ИС, ИТКС, АСУ организации сферы здравоохранения фиксируются в Реестре ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения на праве собственности, аренды или на ином законном основании (Приложение 10).

42. Реестр ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения на праве собственности, аренды или на ином законном основании, подписывается Председателем постоянно действующей комиссии по категорированию и утверждается руководителем организации сферы здравоохранения.

2.7. Оценка задействованности ИС, ИТКС, АСУ в бизнес-процессах

43. Оценка задействованности и влияния ИС, ИТКС, АСУ, которые обрабатывают информацию, необходимую для обеспечения критичных бизнес-процессов организации сферы здравоохранения, и (или) осуществляют управление, контроль или мониторинг критичных бизнес-процессов организации сферы здравоохранения, должна проводиться

применительно к каждой ИС, ИТКС, АСУ, указанной в Реестре ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения на праве собственности, аренды или на ином законном основании. Для каждой такой системы должна быть проведена оценка:

– их задействованности в обработке информации, необходимой для обеспечения критичных бизнес-процессов организации сферы здравоохранения, и (или) осуществлении управления, контроля или мониторинга критичных бизнес-процессов организации сферы здравоохранения;

– их существенного влияния на нарушение или прекращение критичного бизнес-процесса организации сферы здравоохранения, приводящего к негативным социальным, политическим, экономическим, последствиям.

44. Информационная система (ИС) считается задействованной в реализации критичного бизнес-процесса организации сферы здравоохранения, если она предназначена для хранения, поиска и обработки информации, необходимой для выполнения основных функций критичного бизнес-процесса, либо осуществляет управление, контроль или мониторинг критичных бизнес-процессов, либо автоматизирует выполнение бизнес-процессов (технологических операций) и обеспечивает хотя бы одну из следующих функций бизнес-процесса:

– функцию интерпретации данных, заключающуюся в определении смысла данных;

– функцию диагностики оборудования, включающую обнаружение неисправности и отклонений от нормы при выполнении основных функций бизнес-процесса;

– функцию мониторинга интерпретации данных в реальном времени и сигнализации о выходе тех или иных параметров бизнес-процесса за допустимые пределы;

– функцию прогнозирования последствий для бизнес-процесса событий или явлений на основании анализа имеющихся данных;

– функцию планирования действий объектов, выполняющих основные функции бизнес-процесса;

– функцию управления, заключающуюся в поддержании установленного режима деятельности при выполнении бизнес-процесса;

– функцию поддержки принятия решений, заключающуюся в обеспечении необходимой информацией и рекомендациями.

45. Автоматизированная система управления (АСУ) считается задействованной в реализации критичного бизнес-процесса организации сферы здравоохранения, если она предназначена для поддержания установленных режимов технологического процесса, реализуемого бизнес-процессом, за счет контроля и изменения технологических параметров, выдачи команд на исполнительные механизмы и визуального отображения данных о производственном процессе и состоянии технологического оборудования, предупреждения аварийных ситуаций, анализа контролируемых значений, стабилизации режимных параметров и технологических показателей и обеспечивает хотя бы одну из следующих функций бизнес-процесса:

– функцию контроля параметров технологического процесса, реализуемого бизнес-процессом;

– функцию мониторинга соответствия параметров процесса допустимым значениям, информирования персонала при возникновении несоответствий и сигнализации наступления предаварийных и аварийных ситуаций, фиксации времени отклонения параметров процесса за

допустимые пределы (автоматическая), регистрации параметров и записи аварийных и предаварийных ситуаций;

– функцию диагностики оборудования, в том числе, диагностики исправности функционирования самой АСУ;

– функцию управления, контроля или мониторинга технологического или производственного оборудования (исполнительными устройствами) и производимых им процессов, исключения рисков простоев и сбоев работы оборудования.

46. Информационно-телекоммуникационная сеть (ИТКС) считается задействованной в реализации критичного бизнес-процесса организации сферы здравоохранения, если она предназначена для предоставления единого информационного пространства взаимодействия отдельных территориально-распределённых подсистем, реализующих бизнес-процесс организации сферы здравоохранения, и обеспечивает хотя бы одну из следующих функций бизнес-процесса:

– функцию управления и координирования, заключающуюся в администрировании единого информационного пространства и в достижении согласований между различными элементами ИТКС путем установления наиболее рациональных внутренних и внешних связей;

– функцию интеграции информационных ресурсов территориально-распределённых систем;

– функцию обмена информацией (электронная почта, документооборот, обмен сообщениями, передача данных) и предоставления доступа к источникам информации;

– функцию мониторинга, заключающуюся в непрерывном наблюдении, анализе, оценке функционирования ИТКС.

47. При оценке существенного влияния ИС, ИТКС, АСУ на нарушение или прекращение критичного бизнес-процесса организации

сферы здравоохранения учитывается уровень автоматизации функций бизнес-процесса:

– полная автоматизация – реализация бизнес-процесса организации сферы здравоохранения невозможна без участия ИС, ИТКС, АСУ;

– дублирующая автоматизация – бизнес-процесс организации сферы здравоохранения имеет альтернативные (в том числе не автоматизированные) системы управления и обеспечения функций бизнес-процесса.

ИС, ИТКС, АСУ считается оказывающей существенное влияние на нарушение или прекращение критичного бизнес-процесса организации сферы здравоохранения, если его реализация невозможна без участия ИС, ИТКС, АСУ, и отсутствуют альтернативные (не автоматизированные) системы управления и обеспечения функций бизнес-процесса.

ИС, ИТКС, АСУ считается не оказывающей существенного влияние на нарушение или прекращение критичного бизнес-процесса организации сферы здравоохранения, если имеется возможность своевременного обнаружения нарушения штатного режима функционирования ИС, ИТКС, АСУ, задействованной в реализации этого бизнес-процесса, и перехода в течение максимально допустимого периода простоя критичного бизнес-процесса организации сферы здравоохранения на альтернативные (не автоматизированные) системы управления для обеспечения функций бизнес-процесса.

48. В случае, если ИС, ИТКС, АСУ состоит из модулей (подсистем), которые могут обеспечивать относительно самостоятельно функции различных бизнес-процессов организации сферы здравоохранения, оценка может проводиться относительно каждого модуля (подсистемы) отдельно.

49. Алгоритм оценки задействованности и влияния ИС, ИТКС, АСУ на критичные бизнес-процессы организации сферы здравоохранения приведен в Приложении 11.

50. Результаты оценки задействованности и влияния ИС, ИТКС, АСУ на критичные бизнес-процессы организации сферы здравоохранения фиксируются в оценочной части Перечня критичных бизнес-процессов организации сферы здравоохранения (Приложение 8).

2.8. Формирование Перечня потенциально значимых объектов КИИ

2.8.1. Порядок формирования Перечня потенциально значимых объектов КИИ

51. ИС, ИТКС, АСУ считается потенциально значимым объектом КИИ организации сферы здравоохранения, если в результате анализа установлено, что она одновременно задействована в реализации критичного бизнес-процесса и оказывает влияние на нарушение или прекращение критичного бизнес-процесса.

52. ИС, ИТКС, АСУ не считается потенциально значимым объектом КИИ организации сферы здравоохранения и не требует присвоения одной из категорий значимости, установленной постановлением Правительства РФ от 08.02.2018 № 127, если в результате анализа установлено, что она не задействована в реализации критичного бизнес-процесса организации сферы здравоохранения, либо она задействована в реализации критичного бизнес-процесса организации сферы здравоохранения, но не оказывает существенного влияния на нарушение или прекращение критичного бизнес-процесса.

53. ИС, ИТКС, АСУ, задействованная в реализации критичного бизнес-процесса организации сферы здравоохранения, но не оказывающая существенного влияния на нарушение или прекращение критичного бизнес-процесса (дублирующая автоматизация) считается объектом КИИ

организации сферы здравоохранения без присвоения категории значимости, установленной постановлением Правительства РФ от 08.02.2018 № 127.

54. ИС, ИТКС, АСУ, не задействованная в реализации критичного бизнес-процесса, не является объектом КИИ организации сферы здравоохранения.

55. Перечень ИС, ИТКС, АСУ, не требующих присвоения одной из категорий значимости, установленной постановлением Правительства РФ от 08.02.2018 № 127, фиксируется в протоколе работы постоянно действующей комиссии по категорированию.

2.8.2. Согласование Перечня объектов КИИ и отправка в ФСТЭК России

56. На основании заключения об отнесении ИС, ИТКС, АСУ к потенциально значимым объектам КИИ организации сферы здравоохранения формируется и утверждается руководителем организации сферы здравоохранения или уполномоченным лицом Перечень объектов КИИ организации сферы здравоохранения, подлежащих категорированию[26].

57. Форма Перечня объектов КИИ организации сферы здравоохранения, подлежащих категорированию, приведена в Приложении 12.

58. Перечень объектов КИИ организации сферы здравоохранения подлежит согласованию с органами управления государственной и муниципальной системами здравоохранения в части подведомственных им субъектов КИИ.

Согласование осуществляется в произвольной форме. Возможна передача в орган управления государственной или муниципальной системы

[26] Информационное сообщение ФСТЭК России от 17.04.2020 № 240/84/611 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.

здравоохранения запроса на согласование Перечня с приложением предварительно заполненной формы Перечня объектов КИИ, подлежащих категорированию, без утверждающей подписи руководителя организации сферы здравоохранения.

В случае получения от органа управления государственной или муниципальной системы здравоохранения замечаний или корректировок Перечня объектов КИИ, подлежащих категорированию, они должны быть рассмотрены постоянно действующей комиссией по категорированию. По результатам рассмотрения принимается решение о пересмотре Перечня объектов КИИ, подлежащих категорированию, и повторному согласованию с органом управления государственной или муниципальной системой здравоохранения. Отметка о согласовании на итоговом перечне, отправляемом в ФСТЭК России, не требуется.

59. Утвержденный руководителем организации сферы здравоохранения или уполномоченным лицом Перечень объектов КИИ организации сферы здравоохранения, подлежащих категорированию, в течение 5 (пяти) рабочих дней с сопроводительным письмом в произвольной форме направляется в ФСТЭК России[27]с приложением электронной копии Перечня объектов КИИ организации сферы здравоохранения, подлежащих категорированию в формате *.odt, *.ods. Корреспонденция отправляется в законвертованном виде с приложением двух реестров с печатью организации-отправителя.

Образец сопроводительного письма в ФСТЭК России о направлении Перечня объектов КИИ организации сферы здравоохранения, подлежащих категорированию, приведен в Приложении 17.

[27]Адрес: Экспедиция ФСТЭК России, 105066, г. Москва, ул. Старая Басманная, д. 17, 2-е управление ФСТЭК России

2.9. Описание процесса «Категорирование объектов КИИ»

60. Процесс категорирования объектов КИИ организации сферы здравоохранения предполагает проведение расчетов значений критериев значимости объектов КИИ и присвоение в соответствии с полученными результатами одной из категорий значимости или обоснование отсутствия необходимости присвоения объекту КИИ организации сферы здравоохранения категории значимости.

61. Процесс категорирования объектов КИИ организации сферы здравоохранения включает следующие этапы:

– выбор сценария реализации компьютерных атак;

– расчет показателей критериев значимости объектов КИИ организации сферы здравоохранения;

– оформление результатов категорирования объектов КИИ организации сферы здравоохранения.

Состав и содержание этапов процедуры Категорирование объектов КИИ приведены в Приложении 6.

2.10. Выбор сценария реализации компьютерных атак

62. Выбор возможного сценария реализации компьютерных атак проводится на основе анализа возможных действий нарушителей в отношении объектов КИИ организации сферы здравоохранения и угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов. При этом должен быть рассмотрен наихудший сценарий, учитывающий проведение целенаправленных компьютерных атак на потенциально значимые объекты КИИ организации сферы здравоохранения, результатом которых являются прекращение или

нарушение выполнения критичных бизнес-процессов организации сферы здравоохранения и нанесение максимально возможного ущерба[28].

63. При выборе и оценке наихудшего сценария реализации целенаправленной компьютерной атаки для целей определения категории объекта КИИ организации сферы здравоохранения принятые ранее меры обеспечения безопасности потенциально значимого объекта КИИ организации сферы здравоохранения не учитываются.

64. Наихудший сценарий реализации целенаправленной компьютерной атаки предполагает, что нарушитель имеет:

– мотив совершения целенаправленной компьютерной атаки;

– осведомленность о структурно-функциональных характеристиках и особенностях функционирования ИС, ИТКС, АСУ организации сферы здравоохранения;

– осведомленность о мерах защиты информации, применяемых в ИС, ИТКС, АСУ организации сферы здравоохранения, об используемых алгоритмах, аппаратных и программных средствах;

– возможность использовать методы социальной инженерии для изучения поведения пользователей ИС, ИТКС, АСУ организации сферы здравоохранения и их реакции на поступающие к ним внешние данные;

– возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам ИС, ИТКС, АСУ организации сферы здравоохранения для преднамеренного внесения в них программных закладок;

[28] Правила категорирования объектов критической информационной инфраструктуры российской федерации, утв. постановлением Правительства РФ от 08.02.2018 г. № 127, п. 14(1)

– возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения;

– возможность создания методов и средств реализации компьютерных атак с привлечением специализированных научных организаций и реализации компьютерных атак с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в ИС, ИТКС, АСУ организации сферы здравоохранения.

65. Наихудшим сценарием реализации целенаправленной компьютерной атаки признается компьютерная атака, результатом которой для ИС, ИТКС, АСУ организации сферы здравоохранения может быть актуально по крайней мере одно из следующих событий (инцидентов):

– отказ в обслуживании (DoS/DDoS);

– несанкционированный доступ;

– утечка данных (нарушение конфиденциальности);

– модификация (подмена) данных;

– нарушение функционирования технических средств;

– несанкционированное использование вычислительных ресурсов.

Состав возможных событий (инцидентов), которые могут возникнуть в результате реализации наихудшего сценария целенаправленных компьютерных атак и которые необходимо учитывать при оценке значимости объекта КИИ организации сферы здравоохранения применительно к критериям значимости, установленным постановлением Правительства РФ от 08.02.2018 № 127, приведен в Приложении 13.

66. Для событий (инцидентов), которые не могут возникнуть в результате реализации наихудшего сценария целенаправленных

компьютерных атак, оценка значимости объекта КИИ организации сферы здравоохранения применительно к критериям значимости, установленным постановлением Правительства РФ от 08.02.2018 № 127, не проводится.

2.11. Расчет показателей критериев значимости объектов КИИ

2.11.1. Порядок расчета критериев значимости объектов КИИ

67. До начала расчета показателей критериев значимости объекта КИИ организации сферы здравоохранения определяется применимость критериев значимости, установленных постановлением Правительства РФ от 08.02.2018 № 127, для оценки значимости ИС, ИТКС, АСУ организаций сферы здравоохранения.

Обоснования неприменимости критериев значимости, установленных постановлением Правительства РФ от 08.02.2018 № 127 для оценки значимости ИС, ИТКС, АСУ организации сферы здравоохранения, приведены в Приложении 14 (для справки).

68. Для показателей критериев значимости объекта КИИ организации сферы здравоохранения, по которым обоснована их неприменимость, расчет показателей критериев значимости не проводится.

69. Расчет показателей критериев значимости объектов КИИ, установленных постановлением Правительства РФ от 08.02.2018 № 127, проводится для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки[29].

70. Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей), оценка производится по каждому из значений показателя

[29] Допущение: после ликвидации последствий компьютерной атаки предполагается, что существующая система безопасности объекта КИИ восстановлена и не может быть подвержена другой атаке

критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.

71. В случае, если ИС, ИТКС, АСУ организации сферы здравоохранения по одному из показателей критериев значимости отнесена к первой категории, расчет по остальным показателям критериев значимости не проводится.

72. В случае, если ИС, ИТКС, АСУ организации сферы здравоохранения не соответствует ни одному значению показателя критериев значимости, категория значимости объекту КИИ не присваивается.

73. В случае, если функционирование одного объекта КИИ зависит от функционирования другого объекта КИИ, оценка масштаба возможных последствий проводится исходя из предположения о прекращении или нарушении функционирования вследствие компьютерной атаки объекта КИИ, от которого зависит оцениваемый объект.

74. В случае, если ИС, ИТКС, АСУ организации сферы здравоохранения обрабатывают информацию, необходимую для обеспечения нескольких критичных бизнес-процессов организации сферы здравоохранения, и (или) осуществляют управление, контроль или мониторинг нескольких критичных бизнес-процессов организации сферы здравоохранения, оценка показателей критериев значимости производится для каждого критичного бизнес-процесса организации сферы здравоохранения, а категория значимости присваивается по наивысшему значению показателя.

2.11.2. Расчет показателя критерия «Причинение ущерба жизни и здоровью людей»

75. Расчет показателя критерия «Причинение ущерба жизни и здоровью людей[30]» для организации сферы здравоохранения проводится в следующей последовательности:

– на основании регламентов проведения профилактических работ ИС, ИТКС, АСУ, которые обрабатывают информацию, необходимую для обеспечения критичных бизнес-процессов организации сферы здравоохранения, и (или) осуществляют управление, контроль или мониторинг таких критичных бизнес-процессов, определяется максимально допустимый период простоя ($t_{доп}$);

– на основании статистических данных за прошлый пятилетний период определяется усредненное время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$); в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр}$= 10 суток;

– определяется время, в течение которого ИС, ИТКС, АСУ, обрабатывающие информацию, необходимую для обеспечения критичных бизнес-процессов организации сферы здравоохранения, и (или) осуществляющие управление, контроль или мониторинг таких критичных бизнес-процессов, могут быть недоступны (T) по формуле:

$$\boldsymbol{T = t_{устр} - t_{доп}}$$

– на основании статистических данных[31]либо технической документации на ИС, ИТКС, АСУ, а также рассчитанного времени их недоступности (T), определяется максимальное число пациентов, для которых могут быть недоступны ИС, ИТКС, АСУ;

---

[30]Перечень показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений, п. 1, утв. постановлением Правительства РФ от 08.02.2018 № 127

[31] Приказ Росстата от 30.12.2019 № 830 «Об утверждении форм федерального статистического наблюдения с указаниями по их заполнению для организации министерством здравоохранения российской федерации федерального статистического наблюдения в сфере охраны здоровья», Форма № 30.

– полученные данные о максимальном числе пациентов, для которых могут быть недоступны ИС, ИТКС, АСУ организации сферы здравоохранения, сравниваются с показателями, приведенными в пункте 1 Перечня показателей критериев значимости объектов КИИ Российской Федерации и их значений[32], и делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария целенаправленной компьютерной атаки.

2.11.3. Расчет показателя критерия «Отсутствие доступа к государственной услуге»

76. Расчет показателя критерия «Отсутствие доступа к государственной услуге[33]» для организации сферы здравоохранения проводится в следующей последовательности:

– на основании административных регламентов оказания государственных услуг, определяющих период недоступности для оказания услуг, регламентов проведения профилактических работ ИС, ИТКС, АСУ организации сферы здравоохранения, определяется максимально допустимый период простоя ($t_{доп}$);

– на основании статистических данных за прошлый трехлетний период определяется усредненное время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$); в случае отсутствия статистических данных за прошлый трехлетний период, время, требуемое для устранения последствий компьютерной атаки, принимается равным минимально допустимому времени, в течение которого государственная услуга может быть недоступна,

[32] Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утв. постановлением Правительства РФ от 08.02.2018 № 127

[33] Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, п. 5, утв. постановлением Правительства РФ от 08.02.2018 № 127

приведенному в п.5 Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений ($t_{устр}$= 6 часов);

– определяется время, в течение которого государственная услуга может быть недоступна (T) по формуле:

$$\boldsymbol{T = t_{устр} - t_{доп}}$$

– полученный результат расчета сопоставляется с показателями, приведенными в пункте 5 Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, и делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

2.11.4. Оценка показателя критерия «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции»

77. Показатель критерия «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» оценивается по масштабу органа управления государственной или муниципальной системами здравоохранения в деятельности (функционировании) которого задействованы ИС, ИТКС, АСУ организации сферы здравоохранения.

78. Исходя из масштаба государственного органа власти, указанном в пункте 6 Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости

присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

2.11.5. Расчет показателя критерия «Возникновение ущерба субъекту КИИ»

79. Расчет показателя критерия «Возникновение ущерба субъекту критической информационной инфраструктуры[34]» для организаций сферы здравоохранения, имеющих организационно-правовую форму «государственное унитарное предприятие» проводится в следующей последовательности:

– на основании налоговой отчетности и предоставляемых в Федеральную налоговую службу декларациях[35] за предыдущий пятилетний период определяется усредненный суммарный годовой размер выплачиваемых организацией сферы здравоохранения в бюджеты Российской Федерации в соответствии с Налоговым Кодексом Российской Федерации налогов (R_{Σ});

– на основании сведений управленческого и бухгалтерского учета за прошлый пятилетний период определяется усредненный размер годового дохода ($R_{год}$);

– на основании регламентов проведения профилактических работ ИС, ИТКС, АСУ организации сферы здравоохранения определяется максимально допустимый период простоя ($t_{доп}$);

– на основании статистических данных за прошлый пятилетний период определяется усредненное время, требуемое для устранения

[34]Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, п. 9, утв. постановлением Правительства РФ от 08.02.2018 № 127
[35]Приказ ФНС России от 19.10.16 № ММВ-7-3/572@ «Об утверждении формы налоговой декларации по налогу на прибыль организаций, порядка ее заполнения, а также формата представления налоговой декларации по налогу на прибыль организаций в электронной форме

последствий компьютерной атаки ($t_{устр}$); в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр}$= 10 суток;

– ущерб организации сферы здравоохранения от компьютерной атаки ($U_б$) рассчитывается по формуле:

$$U_б = (R_{год} + R_Σ) \times (t_{устр} - t_{доп})$$

– полученный возможный ущерб организации сферы здравоохранения от компьютерной атаки сопоставляется с показателем усредненного размера годового дохода и определяется показатель возможного ущерба по формуле:

$$U_{\%} = U_б / R_{год}$$

– рассчитанный показатель возможного ущерба организации сферы здравоохранения сопоставляется с показателями, приведенными в пункте 8 Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, и делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

2.11.6. Расчет показателя критерия «Возникновение ущерба бюджетам РФ»

80. Расчет показателя критерия «Возникновение ущерба бюджетам Российской Федерации[36]» для организаций сферы здравоохранения, применяющих нулевую ставку по налогу на прибыль[37] и (или) оказывающих медицинские услуги, освобождаемые от налогообложения[38], не проводится.

[36]Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, п. 9, утв. постановлением Правительства РФ от 08.02.2018 № 127
[37] При выполнении условий, перечисленных в ст. 284.1 НК РФ
[38] Ст. 149 НК РФ

81. Для организаций сферы здравоохранения, не применяющих нулевую ставку по налогу на прибыль и (или) не оказывающих медицинские услуги, освобождаемые от налогообложения, на основании налоговой отчетности и предоставляемых в Федеральную налоговую службу декларациях[39] за предыдущий трехлетний период определяется усредненный суммарный годовой размер выплачиваемых организацией сферы здравоохранения в бюджеты Российской Федерации налогов (R_{Σ}) в соответствии с Налоговым Кодексом Российской Федерации.

82. В случае, если для организаций сферы здравоохранения, не применяющих нулевую ставку по налогу на прибыль и (или) не оказывающих медицинские услуги, освобождаемые от налогообложения, усредненный суммарный годовой размер выплачиваемых организацией сферы здравоохранения отчислений в бюджеты Российской Федерации за предыдущий трехлетний период менее 21 300,00 млн. рублей[40], расчет показателя критерия «Возникновение ущерба бюджетам Российской Федерации» не проводится, и постоянно действующей комиссией по категорированию принимается решение об отсутствии необходимости присвоения категории значимости объекту КИИ организации сферы здравоохранения.

При этом, в обосновании отсутствия необходимости присвоения категории значимости объекту КИИ организации сферы здравоохранения указывается, что возможное снижение выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом КИИ (организацией сферы здравоохранения), менее 0,001% от прогнозируемого годового дохода федерального бюджета, усредненного за планируемый трехлетний период с 2019 по 2021 года.

---

[39]Приказ ФНС России от 19.10.16 № ММВ-7-3/572@ «Об утверждении формы налоговой декларации по налогу на прибыль организаций, порядка ее заполнения, а также формата представления налоговой декларации по налогу на прибыль организаций в электронной форме

[40]Сумма в 21 300,00 млн. руб. составляет 0,001% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый трехлетний период с 2020 по 2022 года.

83. Расчет показателя критерия «Возникновение ущерба бюджетам Российской Федерации» для организаций сферы здравоохранения, не применяющих нулевую ставку по налогу на прибыль и (или) не оказывающих медицинские услуги, освобождаемые от налогообложения, и имеющих усредненный суммарный годовой размер выплачиваемых организацией сферы здравоохранения отчислений в бюджеты Российской Федерации за предыдущий трехлетний период более 21 300,00 млн. рублей, проводится в следующей последовательности:

– на основании нормативов, установленных в сфере здравоохранения, определяющих период недоступности для оказания услуг, регламентов проведения профилактических работ ИС, ИТКС, АСУ организации сферы здравоохранения определяется максимально допустимый период простоя ($t_{доп}$);

– на основании статистических данных за прошлый трехлетний период определяется усредненное время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$); в случае отсутствия статистических данных за прошлый трехлетний период принимается $t_{устр}$= 10 суток;

– ущерб бюджетам Российской Федерации от компьютерной атаки ($U_б$) рассчитывается по формуле:

$$U_б = [(R_Σ)/365] \times (t_{устр} - t_{доп})$$

– полученный показатель ущерба бюджетам Российской Федерации от компьютерной атаки сопоставляется с показателем прогнозируемого годового дохода федерального бюджета (R), усредненного за планируемый трехлетний период[41], и определяется показатель возможного ущерба бюджетам Российской Федерации (U%) по формуле:

[41]Прогнозируемый годовой доход федерального бюджета, усредненный за период 2020 – 2022 годы с учетом Федерального закона от 02.12.2019 № 380-ФЗ «О федеральном бюджете на 2020 год и на плановый период 2021 и 2022 годов» принимается равным ***R* = 21 300 млрд. руб**. Актуальные сведения (законы и законопроекты) о прогнозируемом годовом доходе бюджета Российской Федерации доступны на сайте

$$U_{\%} = U_б/R$$

– полученный показатель возможного ущерба бюджетам Российской Федерации сопоставляется с показателями, приведенными в пункте 9 Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, и делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

2.11.7. Расчет показателя критерия «Вредные воздействия на окружающую среду»

84. Расчет показателя критерия «Вредные воздействия на окружающую среду[42]» для организации сферы здравоохранения, использующего источники ионизирующего излучения, проводится в следующей последовательности:

– на основании сведений из Единого государственного реестра недвижимости о границе между субъектами Российской Федерации, границе муниципального образования и границе населенного пункта[43], декларации промышленной безопасности организации сферы здравоохранения, использующей источники ионизирующего излучения, анализа действия поражающих факторов для наиболее опасных по последствиям и вероятных сценариев аварий определяются граница и территория опасной зоны, на которой возможны вредные воздействия на окружающую среду;

официального печатного органа Правительства Российской Федерации https://rg.ru и ли Министерства финансов Российской Федерации https://www.minfin.ru

[42]Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, п. 11, утв. постановлением Правительства РФ от 08.02.2018 № 127

[43] Актуальные сведения о границах о границах инженерной и транспортной инфраструктуры (земли транспорта) доступны на официальном сайте Федеральной службы государственной регистрации, кадастра и картографии или на портале «Госуслуги»

– на основании данных статистических органов о численности населения[44] на начало и конец периода (года) в границах опасной зоны определяется среднеарифметическая численность населения в границах опасной зоны;

– полученные данные о границах опасной зоны сравниваются с показателями, приведенными в пункте 11(а) Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, и определяется потенциальная категория значимости объекта КИИ организации сферы здравоохранения;

– полученные данные о численности населения в границах опасной зоны сравниваются с показателями, приведенными в пункте 11(б) Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, и определяется потенциальная категория значимости объекта КИИ организации сферы здравоохранения;

– из результатов определения потенциальных категорий значимости объекта КИИ организации сферы здравоохранения, полученных по признаку территории (п. 11(а)) и численности населения (п. 11(б)), выбирается наивысшая категория, и делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

[44] Актуальные сведения о численности населения доступны на официальном сайте Федеральной службы государственной статистики Российской Федерации www.gks.ru

2.12. Оформление результатов категорирования объектов КИИ организации сферы здравоохранения

2.12.1. Порядок подготовки заключения о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости

85. Результаты расчета значений показателей критериев значимости объектов КИИ организации сферы здравоохранения для каждой ИС, ИТКС, АСУ организации сферы здравоохранения фиксируются в Протоколе расчетов значений критериев значимости. Форма Протокола расчетов значений критериев значимости приведена в Приложении 15.

86. Протокол расчетов значений критериев значимости объектов КИИ организации сферы здравоохранения оформляется для каждой ИС, ИТКС, АСУ, включенной в Перечень объектов КИИ организации сферы здравоохранения, подлежащих категорированию. Общие сведения об ИС, ИТКС, АСУ, подлежащей категорированию, вносятся в разделы I–III Протокола расчетов значений критериев значимости объектов КИИ.

87. В разделе IV Протокола расчетов значений критериев значимости объектов КИИ в каждой графе, для которой определена неприменимость критериев значимости, установленных постановлением Правительства РФ от 08.02.2018 № 127, указывается обоснование неприменимости критерия.

В форму Протокола расчетов значений критериев значимости объектов КИИ предварительно внесены сведения о неприменимости критериев значимости объектов КИИ с учетом раздела «Допущения и ограничения», Приложений 13 и 14 настоящих методических рекомендаций.

88. В остальных незаполненных графах раздела IV Протокола расчетов значений критериев значимости объектов КИИ указываются результаты расчета значений показателей критериев значимости объектов КИИ организации сферы здравоохранения, описание возможных последствий для бизнес-процесса в результате реализации возможной

компьютерной атаки (инцидента), заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

89. Среди определенных для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки, категорий значимости объекта КИИ организации сферы здравоохранения выбирается наивысшая категория, и в разделе V Протокола расчетов значений критериев значимости объектов КИИ организации сферы здравоохранения делается заключение о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

2.12.2. Оформление Акта категорирования объекта КИИ организации сферы здравоохранения

90. Решение постоянно действующей комиссии по категорированию о присвоении объектам КИИ организации сферы здравоохранения одной из категорий значимости, а также решения об отсутствии необходимости присвоения категорий значимости оформляется Актом, подписывается Председателем постоянно действующей комиссии по категорированию, всеми присутствующими членами постоянно действующей комиссии по категорированию и утверждается исключительно руководителем организации сферы здравоохранения.

91. Акт оформляется на основании Протокола расчетов значений критериев значимости и должен содержать сведения об объекте критической КИИ организации сферы здравоохранения, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Форма Акта приведена в Приложении 16.

92. Допускается оформление единого Акта по результатам категорирования нескольких объектов КИИ для одной организации сферы здравоохранения.

93. Акты о присвоении объектам КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения категорий значимости оформляются в отношении всех объектов КИИ, включенных в Перечень объектов КИИ организации сферы здравоохранения, подлежащих категорированию, направленный в ФСТЭК России.

94. В течение 10 (десяти) рабочих дней со дня утверждения Акта установленным порядком[45]оформляются Сведения о результатах присвоения объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий и с сопроводительным письмом в произвольной форме направляются в ФСТЭК России[46] с приложением электронной копии в формате *.ods. Корреспонденция отправляется в законвертованном виде с приложением двух реестров с печатью организации отправителя.

Акт о присвоении объектам КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии необходимости присвоения категорий значимости оформляется в отношении всех объектов КИИ, и Протоколы расчетов значений критериев значимости в ФСТЭК России не направляются.

Образец сопроводительного письма приведен в разделе II Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17).

[45] Приказ ФСТЭК России от 22.12.2017 № 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»
[46]Адрес: Экспедиция ФСТЭК России, 105066, г. Москва, ул. Старая Басманная, д. 17, 2-е управление ФСТЭК России

2.13. Пересмотр категории значимости объектов КИИ

95. Категория значимости объекта КИИ организации сферы здравоохранения 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 организации сферы здравоохранения и (или) изменением ее организационно-правовой формы.

96. Пересмотр установленной категории значимости или решения об отсутствии необходимости присвоения категории осуществляется не реже чем один раз в 5 лет, а также при изменении показателей критериев значимости.

97. Изменение и пересмотр категории значимости объекта КИИ организации сферы здравоохранения осуществляются в порядке, установленном настоящими методическими рекомендациями для процедуры «Категорирование объектов КИИ».

98. В случае изменения категории значимости объекта КИИ организации сферы здравоохранения сведения о результатах пересмотра категории значимости направляются в ФСТЭК России.

3. РЕКОМЕНДАЦИИ ПО ОФОРМЛЕНИЮ СВЕДЕНИЙ О РЕЗУЛЬТАТАХ КАТЕГОРИРОВАНИЯ

99. Сведения о результатах присвоения объекту КИИ организации сферы здравоохранения одной из категорий значимости либо об отсутствии

необходимости присвоения ему одной из таких категорий (далее – Сведения о результатах категорирования) оформляются для представления в ФСТЭК России в соответствии с установленной формой[47], приведенной в разделе III Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17).

100. Электронные копии Сведений о результатах категорирования оформляются исключительно в формате электронных таблиц OpenDocumentFormat (формат *.ods)[48].

3.1. Исходные данные для оформления сведений

101. Для заполнения формы Сведений о результатах категорирования используются следующие исходные данные:

– выписка из Единого государственного реестра юридических лиц (выписка из Единого государственного реестра индивидуальных предпринимателей);

– локальный нормативный акт (приказ) о назначении уполномоченного лица, на которое возложены функции обеспечения безопасности значимых объектов КИИ в организации сферы здравоохранения[49];

[47] Приказ ФСТЭК России от 22.12.2017 № 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»

[48] Для создания электронных таблиц в формате OpenDocumentFormat используются программное обеспечение StarOffice, OpenOffice или LibreOffice. При отсутствии необходимого программного обеспечения, электронные копии сведений о категорировании создаются с использованием программного обеспечения Exel с последующим переводом в формат *.ods. Для этого после формирования электронной таблицы в формате *.xls (*.xlsx), дается команда «Сохранить как» и в строке «Тип файла» всплывающего окна выбирается строка с записью «Электронная таблица в формате *.ods)

[49] Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказ ФСТЭК России от 21.12.2017 № 235), п. 8

– локальный нормативный акт (приказ) о создании или возложении ответственности за обеспечение безопасности значимых объектов КИИ на структурное подразделение организации сферы здравоохранения[50];

– протокол расчетов значений критериев значимости объекта КИИ организации сферы здравоохранения;

– Акт категорирования объекта КИИ организации сферы здравоохранения;

– Реестр ИС, ИТКС, АСУ (Приложение 10) организации сферы здравоохранения;

– данные бухгалтерского учета организации сферы здравоохранения по разделу «основные средства»;

– данные бухгалтерского учета организации сферы здравоохранения по разделу «нематериальные активы»;

– проектная документация на ИС, ИТКС, АСУ организации сферы здравоохранения;

– данные управленческого учета в подразделении организации сферы здравоохранения, отвечающем за применение информационных технологий и обслуживание средств автоматизации.

3.2. Внесение общих сведений об объектах КИИ и субъектах КИИ

102. Общие сведения об объекте КИИ (п.п. 1.1 – 1.6 формы) вносятся на основании раздела I Протокола расчетов значений критериев значимости.

103. Общие сведения о субъекте КИИ (п.п. 2.1 – 2.6 формы) вносятся на основании выписки из ЕГРЮЛ (ЕГРИП) и локальных нормативных актов.

[50] Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказ ФСТЭК России от 21.12.2017 № 235), п. 10

104. Сведения о лице, эксплуатирующем объект КИИ (п.п. 4.1 – 4.4 формы), вносятся на основании выписки из ЕГРЮЛ (ЕГРИП) и локальных нормативных актов.

105. Адреса размещения объекта КИИ организации сферы здравоохранения, в том числе адреса обособленных подразделений организации сферы здравоохранения, (п. 1.2 формы) и адрес местонахождения организации сферы здравоохранения (п.2.2 формы), адрес местонахождения юридического лица, эксплуатирующего объект КИИ организации сферы здравоохранения (п. 4.2 формы), указываются в следующей последовательности: название улицы, номер дома; название населенного пункта (города, поселка и т.п.); название района; название республики, края, области, автономного округа (области); почтовый индекс[51].

3.3. Внесение сведений о взаимодействии с сетями связи

106. Сведения о взаимодействии объекта КИИ организации сферы здравоохранения и сетей электросвязи вносятся на основании анализа проектной документации на ИС, ИТКС, АСУ организации сферы здравоохранения и данных управленческого учета в подразделении, отвечающем за применение информационных технологий и обслуживание средств автоматизации. При этом, для определения категории сети электросвязи (п. 3.1. формы) допускается использовать сведения о классификации сетей электросвязи, приведенные в IV разделе Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17).

3.4. Внесение сведений о составе объекта КИИ

107. Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ организации сферы здравоохранения (п.п. 5.1

[51]Приказ Министерства связи и массовых коммуникаций РФ от 31.07014 № 234 "Об утверждении Правил оказания услуг почтовой связи"

– 5.4 формы), вносятся на основании данных бухгалтерского учета по разделам «основные средства» и «нематериальные активы», проектной документации на ИС, ИТКС, АСУ организации сферы здравоохранения; данных управленческого учета в подразделении, отвечающем за применение информационных технологий и обслуживание средств автоматизации.

3.5. Внесение сведений об угрозах и возможных последствиях

108. Для целей определения категории значимости объектов КИИ организации сферы здравоохранения разработка Модели угроз и Модели нарушителя не требуется, для этих целей проводится верхнеуровневая оценка угроз безопасности информации. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ организации сферы здравоохранения определяются в следующем порядке:

– на основании раздела IV Протокола расчетов значений критериев значимости для категорируемой ИС, ИТКС, АСУ организации сферы здравоохранения определяется состав возможных событий (инцидентов), которые могут возникнуть в результате реализации наихудшего сценария целенаправленных компьютерных атак;

– на основании определенных возможных событий (инцидентов) с использованием сведений о взаимосвязи возможных угроз безопасности информации и событий (инцидентов) безопасности (раздел V Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17), для категорируемой ИС, ИТКС, АСУ организации сферы здравоохранения выбираются потенциальные угрозы безопасности информации;

– на основе анализа сведений о взаимодействии угроз безопасности информации и объектов воздействия (раздел VI Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) и с

учетом структурно-функциональных характеристик[52] категорируемой ИС, ИТКС, АСУ организации сферы здравоохранения проводится актуализация потенциальных угроз безопасности информации, неактуальные угрозы исключаются;

– на основании полученного перечня актуальных угроз безопасности информации и возможностей нарушителей по реализации угроз безопасности информации (раздел VII Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) определяются типы (категории) возможных нарушителей;

– полученные данные о типе (категории) нарушителя с краткой характеристикой основных возможностей нарушителя по реализации угроз безопасности информации или обоснованием невозможности нарушителем реализовать угрозы безопасности информации вносятся в п. 6.1 формы Сведений о результатах категорирования;

– полученные данные об актуальных угрозах безопасности информации или обоснование их неактуальности вносятся в п. 6.2 формы Сведений о результатах категорирования;

– полученные данные о типах компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, или обоснование невозможности наступления компьютерных инцидентов вносятся в п. 7.1 формы Сведений о результатах категорирования.

Пример определения угроз безопасности информации, нарушителей и последствий от возможных инцидентов приведен в разделе VIII Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17).

[52]Структура и состав системы, физические, логические, функциональные и технологические взаимосвязи.

3.6. Внесение сведений о категории значимости объекта КИИ

109. Сведения о присвоенной объекту КИИ организации сферы здравоохранения категории значимости (п. 8.1 формы) вносятся на основании Акта категорирования объекта КИИ организации сферы здравоохранения.

110. Сведения о значениях показателей значимости объекта КИИ организации сферы здравоохранения и их обоснование (п.п. 8.2 – 8.3 формы) вносятся на основании раздела IV Протокола расчета значений критериев значимости объекта КИИ.

111. При обосновании значений показателей значимости объекта КИИ организации сферы здравоохранения на основании раздела IV Протокола расчета значений критериев значимости объекта КИИ и Приложения 14 вносится информация о неприменимости тех или иных показателей.

3.7. Внесение сведений о принимаемых мерах обеспечения безопасности

112. Сведения об организационных мерах, применяемых для обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения (п. 9.1. формы), вносятся на основании реально выполняемых мероприятий в организации сферы здравоохранения. К организационным мерам могут относиться:

– назначение лица, на которое возложены функции обеспечения безопасности значимых объектов КИИ организации сферы здравоохранения;

– определение структурного подразделения, ответственного за обеспечение безопасности значимых объектов КИИ организации сферы здравоохранения;

– разработка организационно-распорядительных документов организации сферы здравоохранения по безопасности значимых объектов КИИ (регламентов, инструкций, руководств);

– установление контролируемой зоны для объекта КИИ организации сферы здравоохранения;

– контроль физического доступа к объекту КИИ организации сферы здравоохранения.

При внесении сведений об организационно-распорядительных документах организации сферы здравоохранения по безопасности значимых объектов КИИ указываются их названия и регистрационные номера (при наличии). Организационно-распорядительные документы должны соответствовать установленным требованиям[53].

113. При отсутствии в организации сферы здравоохранения организационных мер, применяемых для обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения, в п. 9.1 указываются планируемые к разработке меры и сроки их реализации.

114. Сведения о технических мерах, применяемых для обеспечения безопасности значимого объекта КИИ (п. 9.2. формы), вносятся на основании проектной документации на систему обеспечения безопасности информации объекта КИИ организации сферы здравоохранения, разработанной в соответствии с установленными требованиями[54] (при наличии) или проектной документации на ИС, ИТКС, АСУ организации сферы здравоохранения. К техническим мерам могут быть отнесены следующие меры:

– идентификация и аутентификация;

– управление доступом;

– ограничение программной среды;

– защита машинных носителей информации;

[53] 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», глава IV.
[54] Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита ИС, ИТКС, АСУ и их компонентов.

115. При отсутствии в организации сферы здравоохранения технических мер, применяемых для обеспечения безопасности значимого объекта КИИ, в п. 9.2 указываются планируемые к разработке меры и сроки их реализации.

4. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ ПОСЛЕ ЗАВЕРШЕНИЯ КАТЕГОРИРОВАНИЯ

119. В случае положительного решения Комиссии о присвоении объектам КИИ организации сферы здравоохранения одной из категорий значимости, в соответствии с частью 1 статьи 10 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в целях обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения обязаны создать систему безопасности такого объекта и обеспечить её функционирование в соответствии с требованиями[55], утверждёнными федеральным органом исполнительной власти, уполномоченным в области

[55]«Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утв. приказом ФСТЭК России от 21.12.2017 г. № 235

обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ФСТЭК России).

Кроме того, независимо от результатов категорирования, организации сферы здравоохранения в соответствии с пунктом 1 части 2 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» обязаны организовать взаимодействие с центрами Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и информирования о компьютерных инцидентах. Главным центром ГосСОПКА является Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ).

Состав и последовательность работ по обеспечению безопасности значимых объектов КИИ после завершения категорирования и организации взаимодействия с центрами Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации приведены в Приложении 18.

4.1. Создание системы безопасности значимых объектов КИИ

4.1.1. Общие положения

120. Целью создания системы безопасности значимых объектов КИИ организации сферы здравоохранения является обеспечение их устойчивого функционирования. Средства и методы должны соответствовать категории значимости и быть адекватны для противодействия текущим угрозам.

121. Системы безопасности создаются в отношении всех значимых объектов КИИ организации сферы здравоохранения. Допускается создавать

отдельные системы безопасности для одного или группы значимых объектов КИИ.

122. Системы безопасности объединяют силы обеспечения безопасности значимых объектов КИИ организаций сферы здравоохранения и используемые ими средства обеспечения безопасности значимых объектов КИИ.

К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся подразделения (работники) организации сферы здравоохранения, ответственные за обеспечение безопасности значимых объектов КИИ.

К средствам обеспечения безопасности значимых объектов КИИ организаций сферы здравоохранения относятся программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов КИИ (средства защиты информации), в том числе:

– средства защиты информации от несанкционированного доступа (включая встроенные в системное, прикладное программное обеспечение);
– межсетевые экраны;
– средства обнаружения (предотвращения) вторжений;
– средства антивирусной защиты;
– средства (системы) контроля (анализа) защищенности;
– средства управления событиями безопасности;
– средства защиты каналов передачи данных.

Средства защиты информации значимых объектов КИИ объединяются в подсистему обеспечения безопасности значимых объектов КИИ (систему безопасности).

123. Системы безопасности должны функционировать в соответствии с организационно-распорядительными документами по обеспечению

безопасности значимых объектов КИИ, разрабатываемыми организацией сферы здравоохранения.

124. Состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов КИИ определяет руководитель организации сферы здравоохранения, в том числе определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ (структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ, а также определяет обязанности, возлагаемые на работников структурного подразделения по безопасности, в их должностных регламентах (инструкциях). При этом не допускается возложение на структурное подразделение по безопасности функций, не связанных с обеспечением безопасности значимых объектов КИИ или обеспечением информационной безопасности субъекта КИИ в целом.

125. Создание подсистемы обеспечения безопасности значимых объектов КИИ организации сферы здравоохранения включает следующие этапы:

- планирование;
- реализация;
- контроль.

4.1.2. Структурное подразделение по безопасности

126. Структурное подразделение по безопасности, взаимодействуя с подразделениями (работниками), эксплуатирующими значимые объекты КИИ, либо с привлечением организаций, имеющих лицензию на деятельность по технической защите информации и (или) на деятельность по технической защите конфиденциальной информации, должно:

- разработать необходимые организационно-распорядительные документы по безопасности значимых объектов КИИ;

– провести анализ угроз безопасности информации в отношении значимых объектов КИИ и разработать Модель угроз безопасности информации;

– определить необходимые требования по обеспечению безопасности значимых объектов КИИ и обеспечить реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;

– определить порядок реагирования на компьютерные инциденты в соответствии с пунктом 6 части 4 статьи 6 Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– организовать проведение оценки соответствия значимых объектов КИИ требованиям по безопасности.

127. Для руководителя структурного подразделения по безопасности организации сферы здравоохранения с 01.01.2021 вводятся требования[56] по квалификации и стажу работы:

– наличие высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов)

– наличие стажа работы в сфере информационной безопасности не менее трех лет;

– прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность».

[56]Приказ ФСТЭК России от 27.03.2019 № 64, пп. 4 п.1

128. Для выполнения функций структурного подразделения по безопасности могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

4.1.3. Этап «Планирование» создания подсистемы обеспечения безопасности

129. На этапе «Планирование» устанавливаются требования, которые необходимо выполнить для обеспечения безопасности каждого значимого объекта КИИ организации сферы здравоохранения, и формируется план мероприятий по обеспечению безопасности значимых объектов КИИ. Этап предполагает выполнение следующих процедур:

- выбор мер обеспечения безопасности значимых объектов КИИ;
- проведение GAP-анализа (аудита) ИС, ИТКС, АСУ значимых объектов КИИ;
- планирование мероприятий по обеспечению безопасности значимых объектов КИИ.

Состав процедур этапа «Планирование» создания подсистемы безопасности приведен в Приложении 18.

130. Выбор организационных и технических мер обеспечения безопасности значимых объектов КИИ осуществляется организацией сферы здравоохранения самостоятельно на основе анализа и моделирования угроз безопасности и определения возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения). Подходы, которыми необходимо руководствоваться при моделировании угроз безопасности информации и требования к содержанию Модели угроз, определены ФСТЭК России[57].

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

[57] Приказ ФСТЭК России от 25.12.2017 № 239, п.11.1

В случае, если в организации сферы здравоохранения ранее проводилось моделирование угроз безопасности информации, допускается использование результатов такого моделирования для выбора организационных и технических мер обеспечения безопасности значимых объектов КИИ.

131. Меры по обеспечению безопасности выбираются с учетом угроз безопасности информации в соответствии с разделом III Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации[58].

132. Для выявления уже реализованных обязательных мер по обеспечению безопасности значимого объекта КИИ организации сферы здравоохранения и определения обязательных мер, подлежащих реализации при создании подсистемы обеспечения безопасности, проводится GAP-анализ (аудит) ИС, ИТКС, АСУ значимых объектов КИИ организаций сферы здравоохранения.

При необходимости, для проведения GAP-анализа (аудита) привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации).

При проведении GAP-анализа (аудита) учитываются ранее реализованные меры, установленные требованиями к государственным информационным системам[59], информационным системам персональных данных[60], автоматизированным системам управления производственными и технологическими процессами[61].

133. Меры, подлежащие реализации при создании подсистемы обеспечения безопасности, выявленные в ходе GAP-анализа (аудита),

[58] Утверждены приказом ФСТЭК России от 25.12.2017 г. № 239
[59] Утверждены приказом ФСТЭК России от 11.02.2013 г. № 17
[60] Утверждены приказом ФСТЭК России от 18.02.2013 г. № 21
[61] Утверждены приказом ФСТЭК России от 14.03.2014 № 31

включаются в техническое задание на создание подсистемы обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения. Содержание технического задания определяется п.10 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации[62]. Техническое задание оформляется в соответствии со стандартами[63].

134. В рамках планирования мероприятий по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения в соответствии с установленными требованиями[64] осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов КИИ.

4.1.4. Этап «Реализация» создания подсистемы обеспечения безопасности

135. На этапе «Реализация» осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения[65]. Этап предполагает выполнение следующих процедур:

– разработка организационно-распорядительных документов по безопасности значимых объектов КИИ;

– проектирование подсистемы безопасности значимых объектов КИИ;

– внедрение организационных и технических мер по обеспечению безопасности значимых объектов КИИ.

Состав процедур этапа «Планирование» создания подсистемы безопасности приведен в Приложении 18.

---

[62] Утверждены приказом ФСТЭК Росси иот 25.12.2017 № 239

[63] ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на автоматизированные системы»

[64] «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утв. приказом ФСТЭК России от 21.12.2017№ 235, п.п. 29 - 33

[65] «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утв. приказом ФСТЭК России от 21.12.2017 № 235, п.34

136. Организационно-распорядительные документы, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ организации сферы здравоохранения, а также порядок и правила обеспечения их безопасности, разрабатываются с учетом особенностей деятельности организации сферы здравоохранения, нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры. При этом, положения, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации) организации сферы здравоохранения, а также могут являться частью документов по вопросам функционирования значимого объекта КИИ. Состав и формы организационно-распорядительных документов определяются руководителем организации сферы здравоохранения по предложениям структурного подразделения по безопасности. Организационно-распорядительные документы должны соответствовать установленным требованиям[66].

Организационно-распорядительные документы по безопасности значимых объектов КИИ утверждаются руководителем организации сферы здравоохранения (уполномоченным лицом). По решению руководителя организации сферы здравоохранения отдельные организационно-распорядительные документы по безопасности значимых объектов КИИ могут утверждаться иными уполномоченными на это лицами организации сферы здравоохранения.

Работники организации сферы здравоохранения, эксплуатирующие значимые объекты КИИ, должны быть ознакомлены с положениями организационно-распорядительных документов организации сферы

[66] «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утв. приказом ФСТЭК России от 21.12.2017 № 235, раздел IV

здравоохранения по безопасности значимых объектов КИИ в части, их касающейся.

Перечень рекомендуемых организационно-распорядительных документов по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения приведен в Приложении 19.

137. Проектирование подсистемы безопасности значимого объекта КИИ организации сферы здравоохранения должно осуществляться в соответствии с техническим заданием на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации и категории значимости значимого объекта КИИ организации сферы здравоохранения.

138. В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:

– обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта КИИ организации сферы здравоохранения;

– практическую отработку выполнения средствами защиты информации функций безопасности;

– исключение влияния подсистемы безопасности на функционирование значимого объекта КИИ объекта сферы здравоохранения.

139. Применяемые средства защиты информации должны быть обеспечены гарантийной и/или технической поддержкой со стороны разработчиков (производителей). При этом, в значимом объекте КИИ не допускается техническая поддержка программных и программно-аппаратных средств, в том числе средств защиты информации, зарубежными

организациями, а также организациями, находящимися под прямым или косвенным контролем иностранных физических и (или) юридических лиц[67].

140. Состав и формы рабочей (эксплуатационной) документации определяются в соответствии с техническим заданием на подсистемы обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения. Рабочая (эксплуатационная) документация на значимый КИИ объект должна содержать:

– описание архитектуры подсистемы обеспечения безопасности значимого объекта КИИ организации сферы здравоохранения;

– порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;

– правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

141. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ организуется организацией сферы здравоохранения в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект КИИ и включает:

– установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;

– внедрение организационных мер по обеспечению безопасности значимого объекта КИИ организации сферы здравоохранения;

– предварительные испытания значимого объекта КИИ организации сферы здравоохранения и его подсистемы обеспечения безопасности;

– опытную эксплуатацию значимого объекта КИИ организации сферы здравоохранения и его подсистемы безопасности;

– анализ уязвимостей значимого объекта КИИ организации сферы здравоохранения и принятие мер по их устранению;

---

[67] «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утв. приказом ФСТЭК России от 25.12.2017 № 239, п. 32

– приемочные испытания значимого объекта и его подсистемы безопасности.

142. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ осуществляется в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации[68].

4.1.5. Этап «Контроль» создания подсистемы обеспечения безопасности

143. На этапе «Контроль» осуществляется внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения и эффективности принимаемых организационных и технических мер. По решению руководителя организации сферы здравоохранения может организовываться внешняя оценка с привлечением организаций, имеющих лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации). Этап предполагает выполнение следующих процедур:

– формирование комиссии организации сферы здравоохранения для внутреннего контроля либо выбор внешней организации-аудитора;

– проверка выполнения требований и организационно-распорядительных документов по безопасности значимых объектов КИИ организации сферы здравоохранения;

– инструментальный контроль выполнения технических мер безопасности значимых объектов КИИ организации сферы здравоохранения.

Состав процедур этапа «Контроль» создания подсистемы безопасности приведен в Приложении 18.

144. Контроль проводится ежегодно комиссией, назначаемой руководителем организации сферы здравоохранения. В состав комиссии

[68]Утверждены приказом ФСТЭК России от 25.12.2017 № 239, п. 12 – 12.7

включаются работники структурного подразделения по безопасности, специалисты по безопасности, работники подразделений, эксплуатирующих значимые объекты КИИ, и подразделений, обеспечивающих их функционирование. В состав комиссии могут включаться работники иных подразделений организации сферы здравоохранения.

145. Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности значимых КИИ могут применяться средства контроля (анализа) защищенности.

146. Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем организации сферы здравоохранения (уполномоченным лицом).

На основе замечаний, выявленных по результатам контроля, формируются предложения по совершенствованию безопасности значимых объектов КИИ организации сферы здравоохранения, включаются в ежегодный план мероприятий по обеспечению безопасности значимых объектов КИИ и устраняются в установленные сроки.

4.2. Организация взаимодействия с центрами ГосСОПКА

4.2.1. Общие положения

147. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) обеспечивает сбор, накопление, систематизацию и анализ информации, получаемой от субъектов критической информационной инфраструктуры. Основным назначением ГосСОПКА является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

148. Основной организационно-технической составляющей ГосСОПКА являются центры обнаружения, предупреждения и ликвидации

последствий компьютерных атак (далее – Центры), организованные по ведомственному и территориальному принципам. Главным центром является Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Министерство здравоохранения Российской Федерации может создать ведомственный Центр ГосСОПКА.

Общая структура Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) приведена в Приложении 20.

149. В рамках взаимодействия с ГосСОПКА организация сферы здравоохранения имеет право:

– получать информацию об угрозах безопасности информации, обрабатываемой объектами критической информационной инфраструктуры, функционирующими в сфере здравоохранения, и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах КИИ;

– получать информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

– за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

150. Организации сферы здравоохранения обязаны незамедлительно информировать о компьютерных инцидентах НКЦКИ в установленном порядке[69].

[69] Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ Российской Федерации, между субъектами КИИ Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

151. Организация взаимодействия с ГосСОПКА предполагает выполнение следующих процедур:

– выбор центра ГосСОПКА, заключение договора;

– уведомление НКЦКИ о вхождении в зону ответственности центра ГосСОПКА;

– разработку Регламентов взаимодействия и реагирования;

– организацию сбора информации об инцидентах ИБ.

Состав процедур организации взаимодействия с ГосСОПКА приведен в Приложении 18.

4.2.2. Выбор Центра ГосСОПКА

152. Организация сферы здравоохранения может организовать взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

– непосредственно через НКЦКИ;

– через ведомственный Центр ГосСОПКА Министерства здравоохранения Российской Федерации, взаимодействующий с НКЦКИ (при условии его создания);

– через коммерческие (корпоративные) центры ГосСОПКА, созданные на территории региона расположения организации сферы здравоохранения.

153. Взаимодействие организации сферы здравоохранения с Центрами ГосСОПКА осуществляется на договорной основе. После заключения договора на обслуживание с выбранным Центром ГосСОПКА организация сферы здравоохранения уведомляет НКЦКИ о вхождении в зону ответственности центра ГосСОПКА.

154. Взаимодействие организации сферы здравоохранения с Центром ГосСОПКА осуществляется в рамках разрабатываемого Регламента взаимодействия.

4.2.3. Организация сбора и обмена информацией о компьютерных инцидентах

155. Обязательным для организации сферы здравоохранения является обмен информацией о компьютерных инцидентах с НКЦКИ[70] и создаваемым ведомственным Центром ГосСОПКА Министерства здравоохранения Российской Федерации (при условии его создания). Круг иных субъектов КИИ, с которыми осуществляется такой обмен, организации сферы здравоохранения определяют самостоятельно. При направлении информации о компьютерных инцидентах в ведомственный Центр ГосСОПКА Министерства здравоохранения Российской Федерации (при условии его создания) организации сферы здравоохранения обязаны параллельно информировать об этом НКЦКИ.

156. Обмен информацией о компьютерных инцидентах осуществляется в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. Обмен информацией о компьютерных инцидентах осуществляется путем направления уведомлений в соответствии с установленными форматами[71].

157. Взаимодействие с НКЦКИ возможно следующими способами:

– с использованием технической инфраструктуры НКЦКИ (при наличии подключения), предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ;

---

[70] Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»

[71] Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

– посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в сети «Интернет» по адресу: http://cert.gov.ru .

158. Состав информации, передаваемой в рамках взаимодействия с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), приведен в Приложении 21.

Приложение 1.

Термины и определения, используемые в настоящих методических рекомендациях

В данном документе используются термины и определения, установленные Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также национальными стандартами, и адаптированные для организаций сферы здравоохранения, в частности:

Термины и определения

Автоматизированная система управления	комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами
Бизнес-процесс	совокупность взаимосвязанных мероприятий или работ, направленных на выполнение функций (полномочий) или осуществления видов деятельности организации сферы здравоохранения (аналогично понятию управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, изложенному в п.5 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утв. постановлением Правительства Российской Федерации от 08.02.2018 г. № 127)
Воздействие на окружающую среду	ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия

Государственные информационные системы	федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов
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
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационно-телекоммуникационная сеть	технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники
Категорирование объектов критической информационной инфраструктуры	процесс определения категорий значимости объектов критической информационной инфраструктуры, обеспечивающих управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности организаций сферы здравоохранения, на основании показателей критериев значимости объектов критической информационной инфраструктуры и их значений, установленных Правительством Российской Федерации
Компьютерная атака	целенаправленное воздействие программных и(или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации
Компьютерный	факт нарушения и (или) прекращения

инцидент	функционирования объекта критической информационной инфраструктуры организации сферы здравоохранения, 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	объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов
Максимально допустимый период простоя	период, по истечении которого критичный бизнес-процесс может полностью прекратиться или произойдет отклонение значений параметров критичного бизнес-процесса, в том числе временных параметров и параметров надежности, от проектных (штатных) режимов функционирования, превышающих установленные допуски
Мониторинг критичных бизнес-процессов	постоянное (регулярное) наблюдение за значениями характеристик критичного бизнес-процесса
Нарушение критичного процесса	отклонение значений параметров критичного бизнес-процесса организации сферы здравоохранения, в том числе временных параметров и параметров надежности, от проектных (штатных) режимов функционирования
Обработка информации, необходимой для критичных бизнес-процессов	систематическое выполнение операций над данными, необходимыми для обеспечения критичного бизнес-процесса
Объект обеспечения жизнедеятельности населения	Объекты водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения
Объекты критической информационной инфраструктуры	информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления организаций сферы здравоохранения
Прекращение	полное прекращение выполнения критичного

критичного процесса	бизнес-процесса организации сферы здравоохранения
Производственный бизнес-процесс	любой процесс в деятельности организации сферы здравоохранения, направленные на достижение конечного результата выполняемых функций (полномочий) или видов деятельности организации сферы здравоохранения. Производственные процессы являются линейными процессами на выходе которых предполагается определенный результат
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 (применительно к организациям, осуществляющим деятельность в сфере охраны здоровья – организациям сферы здравоохранения)	федеральные органы исполнительной власти в сфере охраны здоровья и их территориальные органы, исполнительные органы государственной власти субъектов Российской Федерации в сфере охраны здоровья, органы местного самоуправления муниципальных районов и городских округов, осуществляющие полномочия в сфере охраны здоровья, федеральные органы исполнительной власти в сфере охраны здоровья и их территориальные органы, лечебные медицинские организации, медицинские организации особого типа, медицинские организации по надзору сферы защиты прав потребителей и благополучия человека в соответствии с действующей номенклатурой, утвержденной Приказом Минздрава России от 06.08.2013 № 529н, а также организации, осуществляющие фармацевтическую деятельность и создаваемые юридическими и физическими лицами медицинские организации, фармацевтические организации и иные организации частной системы здравоохранения, осуществляющие деятельность в сфере охраны здоровья.
Технологический бизнес-процесс	любой процесс в деятельности организации сферы здравоохранения, который обслуживает основные бизнес-процессы, направленные на выполнение функций (полномочий) или осуществление видов деятельности организации сферы здравоохранения

Управление критичным бизнес-процессом	поддержание критичного бизнес-процесса в рабочем состоянии в рамках заданных значений характеристик критичного бизнес-процесса
Управленческий бизнес-процесс	любой процесс в деятельности организации сферы здравоохранения, направленный на управление выполнением функций (полномочий) или осуществления видов деятельности организации сферы здравоохранения. Управленческие бизнес-процессы представляют собой совокупность циклических действий, связанных с выявлением проблем, поиском и организацией выполнения принятых решений для управляемых объектов
Финансово-экономический бизнес-процесс	любой процесс в деятельности организации сферы здравоохранения, связанный с экономическими, финансово-денежными, учетными, фискальными аспектами деятельности организации сферы здравоохранения, а также с обеспечением текущей деятельности организации сферы здравоохранения посредством реализации финансовых прав и исполнения финансовых обязательств
Целенаправленная компьютерная атака	компьютерная атака, адаптированная к структурно-функциональным характеристикам интересующей нарушителя информационной системы, информационно-телекоммуникационной сети, автоматизированной системы управления

Сокращения

АСУ	Автоматизированные системы управления
ГИС	Государственные информационные системы
ЕГИСЗ	Единая государственная информационная система в сфере здравоохранения
ЕГРЮЛ	Единый государственный реестр юридических лиц
ЕГРИП	Единый государственный реестр индивидуальных предпринимателей
ИС	Информационная система
ИТКС	Информационно-телекоммуникационная система
КИИ	Критическая информационная инфраструктура
МИС	Медицинская информационная система
МИС МО	Медицинские информационные системы медицинских организаций
НМО	Надзорные медицинские организации

ОУЗ	Органы государственной власти субъектов РФ в сфере охраны здоровья
ФО	Организации, независимо от организационно-правовой формы осуществляющие фармацевтическую деятельность (организация оптовой торговли лекарственными средствами, аптечная организация)
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Приложение 2.

Перечень основных нормативных правовых актов, использованных при разработке настоящих методических рекомендаций

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

2. Постановление Правительства РФ от 26.06.2012 № 644 «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов»;

3. Постановление 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»;

4. Постановление Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»;

5. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;

6. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

7. Приказ ФСТЭК России от 22.12.2017 № 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»;

8. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

9. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

10. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

11. ФСТЭК России. Информационное сообщение от 17.04.2020 № 240/84/611 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.

Приложение 3.

Перечень организаций сферы здравоохранения, на которые распространяется область действия настоящих методических рекомендаций

Рекомендации по проведению процесса категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере здравоохранения, изложенные в настоящих методических рекомендациях, предназначены для организаций сферы здравоохранения (субъектов КИИ) к которым относятся:

I. Органы управления системой здравоохранения, в том числе:

– федеральные органы исполнительной власти в сфере охраны здоровья и их территориальные органы;

– исполнительные органы государственной власти субъектов Российской Федерации в сфере охраны здоровья;

– органы местного самоуправления муниципальных районов и городских округов, осуществляющие полномочия в сфере охраны здоровья.

II. Лечебные организации сферы здравоохранения в соответствии с действующей номенклатурой, утвержденной Приказом Минздрава России от 06.08.2013 № 529н, в том числе:

– больницы;

– родильные дома;

– госпитали;

– медико-санитарные части;

– дома (больницы) сестринского ухода;

– хосписы;

– лепрозории;

– диспансеры;

– амбулатории;

– поликлиники;

- женские консультации;
- дома ребенка;
- молочные кухни;
- центры скорой медицинской помощи и переливания крови;
- санаторно-курортные организации.

III. Медицинские организации особого типа в соответствии с действующей номенклатурой, утвержденной Приказом Минздрава России от 06.08.2013 № 529н, в том числе:

- медицинские центры (профилактики, медицины катастроф, «Резерв», информационно-аналитический, биофизический, военно-врачебной экспертизы, судебно-медицинской экспертизы);
- бюро (медико-социальной экспертизы, медицинской статистики, патологоанатомическое, судебно-медицинской экспертизы);
- лаборатории (клинико-диагностические, бактериологические);
- медицинские воинские формирования (медицинские отряды, отдельные медицинские батальоны).

IV. Медицинские организации по надзору в сфере защиты прав потребителей и благополучия человека в соответствии с действующей номенклатурой, утвержденной Приказом Минздрава России от 06.08.2013 № 529н, в том числе центры (станции):

- гигиены и эпидемиологии;
- противочумные;
- дезинфекционные;
- гигиенического образования населения;
- государственного санитарно-эпидемиологического надзора.

V. Организации, осуществляющие фармацевтическую деятельность (оптовая торговля лекарственными средствами, хранение лекарственных средств и препаратов, перевозка лекарственных средств и препаратов,

розничная торговля лекарственными препаратами, отпуск лекарственных препаратов, изготовление лекарственных препаратов для медицинского применения).

VI. Создаваемые юридическими и физическими лицами медицинские организации, фармацевтические организации и иные организации частной системы здравоохранения, осуществляющие деятельность в сфере охраны здоровья.

Приложение 4.

Примеры информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере здравоохранения

Примеры ИС, ИТКС, АСУ, которые в рамках настоящих методических рекомендаций могут быть рассмотрены независимо друг от друга и отнесены к отдельным объектам КИИ организации сферы здравоохранения:

№	ИС, АСУ, ИТКС	КЛАСС
1.	Федеральные государственные информационные системы в сфере здравоохранения, в том числе: Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ)	ИС
2.	Государственные информационные системы сферы здравоохранения субъектов Российской Федерации (ГИС субъектов Российской Федерации), в том числе с учетом централизованных систем (подсистем)	ИС
3.	Медицинские информационные системы медицинских организаций (МИС)	ИС
4.	Информационные системы фармацевтических организаций	ИС
5.	Защищенные сети передачи данных	ИТКС
6.	АСУ технологических процессов лечения пациентов	АСУ
7.	Медицинские комплексы программно-аппаратные , например: – системы функциональной диагностики; – системы оперативного слежения за состоянием пациента (системы мониторинга); – системы хранения и обработки медицинских изображений; – системы лабораторной диагностики; – биотехнические системы замещения жизненно важных функций организма и протезирования и др.	АСУ
8.	Автоматизированные системы диагностики заболеваний и прогнозирования результатов их лечения, например: – компьютерные диагностические системы (вероятностные, консультативные, скрининговые и экспертные) и др.	ИС/АСУ

№	ИС, АСУ, ИТКС	КЛАСС
9.	Медицинские информационно-справочные системы	ИС

Приложение 5.

Рекомендации по формированию постоянно действующей комиссии по категорированию объектов КИИ организации сферы здравоохранения

Согласно Правилам категорирования объектов критической информационной инфраструктуры Российской Федерации[72]категорирование объектов КИИ осуществляется организацией сферы здравоохранения самостоятельно, для чего локальным правовым актом (приказом) руководителя организации сферы здравоохранения создается постоянно действующая комиссия по категорированию объектов КИИ (далее – Комиссия)[73].

Состав Комиссии

Комиссию возглавляет председатель, в качестве которого выступает руководитель организации сферы здравоохранения или уполномоченное им лицо[74]. При создании Комиссии необходимо учитывать высокую ответственность председателя Комиссии в определении категории значимости объектов КИИ, необходимость привлечения экспертов из различных областей деятельности, а также постоянный характер деятельности Комиссии. Исходя из этого, уполномоченное лицо должно быть наделено определенными полномочиями, а его должностные обязанности должны быть закреплены в порядке, установленном трудовым законодательством[75].

Членами Комиссии назначаются эксперты из числа наиболее квалифицированных работников организации сферы здравоохранения, являющихся специалистами в области осуществляемых видов деятельности,

[72] Утверждены постановлением Правительства Российской Федерации от 08.02.2018 № 127, п. 2
[73] Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утв. постановлением Правительства Российской Федерации от 08.02.2018 № 127, п. 11
[74] Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утв. постановлением Правительства Российской Федерации от 08.02.2018 № 127, п. 13
[75] Трудовой кодекс Российской Федерации, ст. 60.2

информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования. В качестве экспертов рекомендуется привлекать специалистов, деятельность которых связана с обработкой информации в ИС, ИТКС, АСУ организации сферы здравоохранения, а также специалистов, имеющие квалификацию и опыт работы в области применения информационных технологий и (или) в области защиты информации.

При привлечении в качестве экспертов специалистов от подразделений организации сферы здравоохранения по защите информации рекомендуется привлекать лиц, имеющих высшее образование или прошедших переподготовку (повышение квалификации) по направлению подготовки «Информационная безопасность».

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения.

Допускается по решению руководителя организации сферы здравоохранения или уполномоченного лица, для оценки критичности бизнес-процессов, выявления задействованности ИС, ИТКС, АСУ в критичных бизнес-процессах организации сферы здравоохранения привлекать экспертов сторонних организаций, в том числе организаций, имеющих соответствующие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации. При этом, не допускается передавать внешним экспертам право принятия решения о присвоении объекту КИИ организации сферы здравоохранения одной из категорий значимости либо решения об отсутствии необходимости присвоения им категорий значимости. Привлекаемые эксперты не являются членами Комиссии.

Форма локального нормативного акта о создании Комиссии

Создание комиссии необходимо оформить локальным нормативным актом (приказом), в котором определяется состав Комиссии, вводится Положение о постоянно действующей комиссии, порядок хранения документов Комиссии.

При назначении председателем Комиссии уполномоченного лица, в локальном нормативном акте должны быть отражены его полномочия.

Локальный нормативный акт (приказ) о создании Комиссии оформляется в соответствии с правилами документооборота, принятыми в организации сферы здравоохранения.

<полное наименование организации сферы здравоохранения>

ПРИКАЗ

(проект)

«__» _____ 20__ г. _____№ _____

_____

(наименование населенного пункта)

О создании постоянно действующей комиссии по категорированию объектов КИИ (наименование организации сферы здравоохранения)

Во исполнения пункта 11 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 г. № 127, в целях организации проведения работ по категорированию объектов критической информационной инфраструктуры в *<полное наименование организации сферы здравоохранения>*

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры в *<полное наименование организации сферы здравоохранения>*.

2. Утвердить состав постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры согласно приложению № 1 к приказу.

3. Утвердить Положение о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры *<полное наименование организации сферы здравоохранения>*.

4. Комиссии организовать работу по категорированию объектов критической информационной инфраструктуры *<полное наименование организации сферы здравоохранения>* в строгом соответствии с

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.

5. Контроль за исполнением настоящего приказа оставляю за собой.

_____ _____ _____

_____ _____ _____

(должность) *(подпись)* *(Ф. И. О.)*

Приложение № 1
к приказу
<полное наименование организации сферы здравоохранения>
от « » 20__ г. № _____

СОСТАВ ПОСТОЯННО ДЕЙСТВУЮЩЕЙ КОМИССИИ
<полное наименование организации сферы здравоохранения>
по категорированию объектов КИИ

Председатель комиссии:

(ФИО) – _____,
(должность)

Секретарь комиссии:

(ФИО) – _____,
(*должность*)

Члены комиссии:

(ФИО) – _____,
(*должность*)

(ФИО) – _____,
(*должность*)

(ФИО) – _____,
(*должность*)

(ФИО) – _____.
(*должность*)

Приложение № 2
к приказу
<полное наименование организации сферы здравоохранения>
от «» 20__ г. № _____

Положение о постоянно действующей комиссии по категорированию объектов КИИ
<полное наименование организации сферы здравоохранения>
(проект)

1. Положение о комиссии по категорированию объектов критической информационной инфраструктуры (далее – Комиссия) определяет задачи, функции Комиссии, ее права и порядок организации ее деятельности.

2. Комиссия создается для организации работ по категорированию объектов КИИ <*наименование организации сферы здравоохранения*>.

3. Комиссия является постоянно действующим консультативно-совещательным органом.

4. Комиссия в своей деятельности руководствуется федеральными законами, актами Президента Российской Федерации, Правительства Российской Федерации, в том числе Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 № 127, приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 22.12.2017 № 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» и настоящим Положением.

5. Состав Комиссии устанавливается приказом по Организации.

6. Комиссия выполняет следующие функции:

6.1. определение бизнес-процессов, в рамках выполнения функций (полномочий) или осуществления видов деятельности <*наименование организации сферы здравоохранения*>, как субъекта КИИ;

6.2. выявление критичных бизнес-процессов <*наименование организации сферы здравоохранения*>;

6.3. выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критичных бизнес-процессов, и (или) осуществляют управление, контроль или мониторинг критичных бизнес-процессов, подготовка предложений для включения в перечень объектов КИИ, подлежащих категорированию;

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

6.5. анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ <*наименование организации сферы здравоохранения*>;

6.6. оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;

6.7. расчет показателей значимости для объектов КИИ;

6.8. присвоение каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости.

7. Организация деятельности Комиссии.

7.1. Заседания Комиссии проводятся по мере необходимости.

7.2. Решение о проведении заседаний Комиссии принимается председателем Комиссии на основании предложений членов Комиссии.

7.3. Заседания Комиссии проводятся в случае присутствия не менее 50% численного состава постоянных членов Комиссии. Присутствие на заседании Комиссии иных лиц, кроме членов Комиссии, допускается с разрешения председателя Комиссии. В случае отсутствия председателя Комиссии, его полномочия осуществляет один из членов Комиссии, назначенный Председателем Комиссии. При отсутствии кворума заседание Комиссии переносится на другую дату, определяемую Председателем Комиссии.

7.4. Все решения по рассматриваемым Комиссией вопросам принимаются открытым голосованием простым большинством голосов членов Комиссии. При голосовании каждый член Комиссии имеет один голос. При равенстве голосов решающим голосом является голос Председателя Комиссии.

7.5. Решение Комиссии о включении объектов КИИ, <*наименование организации сферы здравоохранения*>, в перечень объектов КИИ, подлежащих категорированию, оформляется Протоколом Комиссии, подписывается всеми присутствующими членами Комиссии и утверждается Председателем Комиссии.

7.6. Решение Комиссии о присвоении объектам КИИ <*наименование организации сферы здравоохранения*> одной из категорий значимости, а также решения об отсутствии необходимости присвоения категорий значимости оформляется Актом, подписывается Председателем Комиссии, всеми присутствующими членами Комиссии и утверждается руководителем <*наименование организации сферы здравоохранения*>.

7.7. Срок подписания проекта Акта Комиссии членом Комиссии не может превышать двух рабочих дней с даты его получения от Секретаря

Комиссии. Подписанный членами Комиссии акт Комиссии, направляются Секретарем Комиссии не позднее двух календарных дней Председателю Комиссии на утверждение.

7.8. Акт оформляется с учетом пункта 16 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 № 127 и должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Допускается оформление единого акта по результатам категорирования нескольких объектов КИИ, принадлежащих <*наименование организации сферы здравоохранения*>.

7.9. В течение 10 рабочих дней со дня утверждения Акта, указанного в пункте 7.7 настоящего Положения, сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий направляются в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ.

7.10.По результатам заседания Комиссии, помимо решений, указанных в пунктах 7.5, 7.6 настоящего Положения, могут приниматься иные решения Комиссии, которые должны быть отражены в Протоколе Комиссии.

8. Председатель Комиссии:

8.1. несет ответственность за соблюдение установленных сроков проведения категорирования;

8.2. организует работу Комиссии;

8.3. назначает дату, время и место проведения заседаний Комиссии;

8.4. утверждает повестку заседания Комиссии;

8.5. руководит заседанием Комиссии;

8.6. распределяет обязанности между членами Комиссии;

8.7. пользуется правами члена Комиссии при голосовании;

8.8. имеет право:

8.8.1. привлекать для решения частных задач работников <*наименование организации сферы здравоохранения*>, экспертов сторонних организаций, представителей вышестоящих организаций (без права голоса);

8.8.2. отдавать распоряжения в пределах установленных полномочий, обязательные для исполнения всеми работниками <*наименование организации сферы здравоохранения*>.

9. Секретарь Комиссии:

9.1. координирует деятельность членов Комиссии;

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

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

9.4. совместно с членами Комиссии готовит информацию, документы, иные материалы к заседаниям Комиссии;

9.5. ведет протокол заседания Комиссии;

9.6. в течение 3 рабочих дней с даты проведения заседания Комиссии и в соответствии с ее решением готовит итоговые документы и представляет их на подпись председателю Комиссии и членам Комиссии;

9.7. организует и ведет делопроизводство Комиссии и обеспечивает сохранность документов Комиссии;

9.8. осуществляет организационно-техническое обеспечение деятельности Комиссии.

10. Члены Комиссии:

10.1.лично участвуют в заседании Комиссии;

10.2. участвуют в обсуждении вопросов, включенных в повестку заседания Комиссии;

10.3.знакомятся с информацией, документами и материалами по вопросам, вынесенным на обсуждение Комиссии на стадии их подготовки, вносят свои предложения;

10.4. имеют право формировать запросы о получении информации, необходимой для работы Комиссии;

10.5.в случае несогласия с принятым решением излагают свое особое мнение в письменном виде, которое прилагается к соответствующему Протоколу Комиссии.

11. Проекты заключений и актов Комиссии, не позднее 5 календарных дней со дня проведения заседания, направляются Секретарем Комиссии всем членам Комиссии на подписание, за исключением Председателя Комиссии.

12. Протоколы Комиссии и Акты должны храниться в <*наименование организации сферы здравоохранения*> до вывода из эксплуатации объекта КИИ или до пересмотра ранее установленной категории значимости.

13. Не реже чем один раз в 5 лет Комиссия осуществляет пересмотр установленной категории значимости в соответствии с настоящим Положением. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный

орган, уполномоченный в области обеспечения безопасности КИИ (ФСТЭК России).

14. Организационное и материально-техническое обеспечение деятельности Комиссии осуществляется за счет средств <*наименование организации сферы здравоохранения*>.

15. Комиссия подлежит расформированию в случаях:

15.1. прекращения <*наименование организации сферы здравоохранения*> выполнения функций (полномочий) или осуществления видов деятельности в сфере здравоохранения;

15.2. ликвидации, реорганизации <*наименование организации сферы здравоохранения*> и (или) изменения его организационно-правовой формы, в результате которых были утрачены признаки субъекта КИИ.

С приказом ознакомлены:

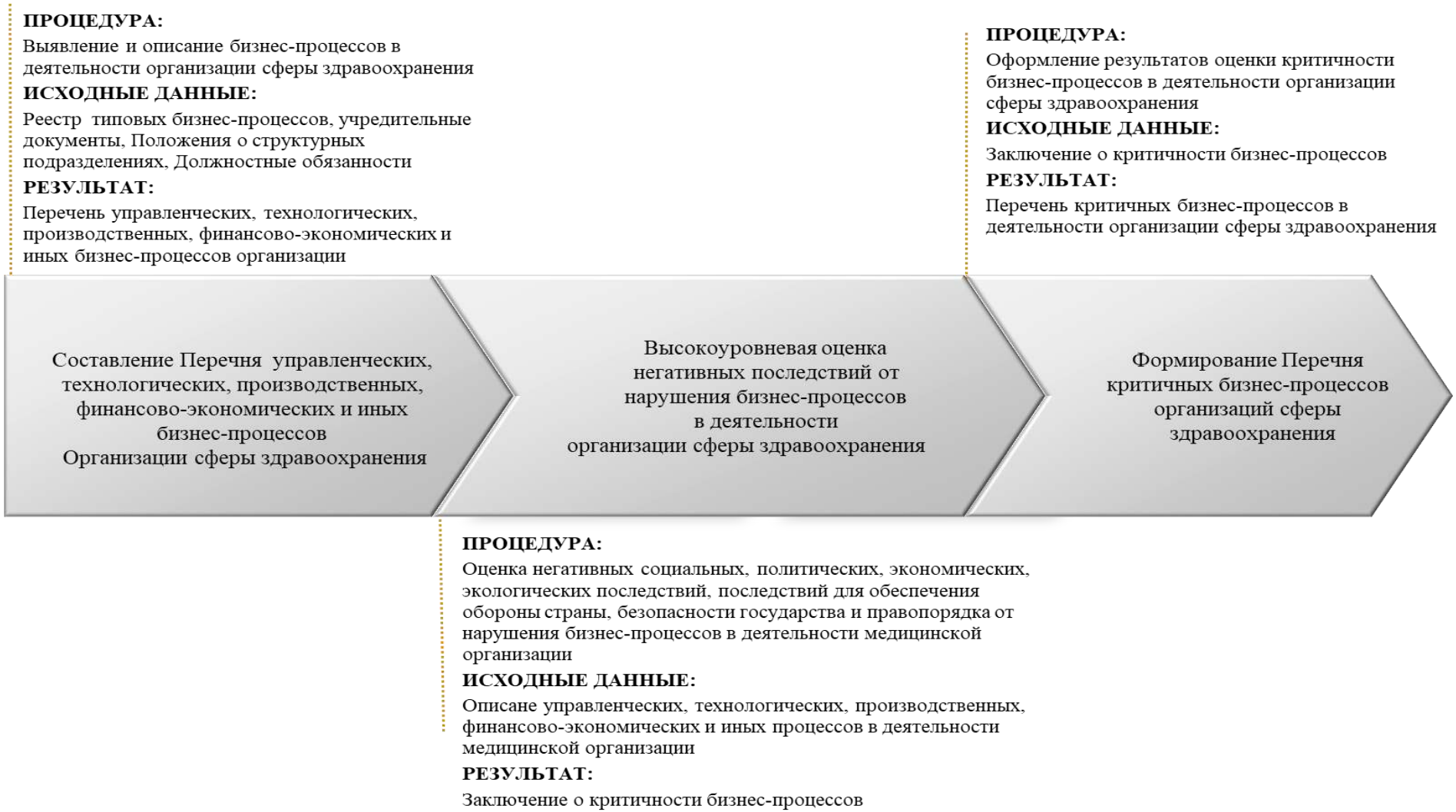
(наименование должности)	(Ф.И.О.)
(наименование должности)	(Ф.И.О.)
(наименование должности)	(Ф.И.О.)

Приложение 6.

Состав процессов, осуществляемых при категорировании объектов КИИ организации сферы здравоохранения

Содержание процессов, осуществляемых при категорировании объектов КИИ

Содержание этапов процесса определения бизнес-процессов организации сферы здравоохранения



Содержание этапов процесса определения и формирования Перечня объектов КИИ организации сферы здравоохранения

Содержание этапов процесса категорирования объектов КИИ организации сферы здравоохранения

Приложение 7.

Форма Реестра бизнес-процессов организации сферы здравоохранения

Образец Реестра бизнес-процессов

УТВЕРЖДАЮ

_____

(должность руководителя организации сферы здравоохранения)

_____

(Ф.И. О.)

« » _____ 20__ г.

РЕЕСТР
бизнес-процессов
<полное наименование организации сферы здравоохранения>

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
Управленческие	–								
	–								
	–								
Технологические	–								
	–								

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	–								
Производственные	–								
	–								
	–								
Финансово-экономические	–								
	–								
	–								
Иные	–								
	–								
	–								

Председатель постоянно действующей Комиссии по категорированию объектов КИИ
<полное наименование организации сферы здравоохранения.>

_____
(Ф.И. О.)

«___» _____ 20___ г

Пример заполнения формы Реестра бизнес-процессов

РЕЕСТР
бизнес-процессов
<полное наименование организации сферы здравоохранения>

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
Управленческие	– информационно-аналитическая деятельность	Предполагает: сбор, хранение, обработку и представление информации, необходимой поддержки принятия управленческих решений по вопросам развития здравоохранения, сбор и агрегацию первичных данных, проведение экономического и предметного анализа, подготовку отчетности и медицинской статистики информационное обеспечение медицинского персонала клинической, научной, нормативной, юридической, оперативной, обзорно-аналитической, прогностической информацией сбор, консолидацию и обработку транзакционных данных медицинских информационных систем (данных первичного учета в здравоохранении)	ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к принятию ошибочных управленческих решений в сфере ответственности государственного органа власти, что может негативно повлиять на реализацию его функций (полномочий).	Критичный
	– ведение регистров	Предполагает: сбор, хранение, обработку и представление	ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к принятию	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
		информации, необходимой для информационной поддержки управления деятельностью в сфере охраны здоровья граждан, включая информацию о медицинских и фармацевтических организациях						государственным органом власти ошибочных управленческих решений	
	– административно-управленческая деятельность	Предполагает: управление деятельностью организации сферы здравоохранения для достижения ее эффективного функционирования организацию совместной работы коллектива организации сферы здравоохранения по решению стоящих перед ним задач материальный учет лекарственных средств и товаров аптечного ассортимента, продуктов питания, изделий медицинского назначения, комплекса технических средств, медицинского оборудования	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не может привести к причинению ущерба жизни и здоровью людей, либо к прекращению или нарушению функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Некритичный
	– клинико-экспертная деятельность	Предполагает оценку: состояния здоровья пациентов, определение соответствия их здоровья и условий жизнедеятельности существующим правовым положениям и социальным льготам, возможности осуществлять отдельные виды деятельности качества (эффективности) медицинского обслуживания и медицинской помощи результатов лечебно-диагностического процесса и показателей здоровья населения	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не может привести к причинению ущерба жизни и здоровью людей, либо к прекращению или нарушению функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	–								
	–								
Технологические	– Реализация межведомственного взаимодействия	Реализует функции информационного взаимодействия: с другими ведомствами в рамках процессов исполнения государственных и муниципальных функций между медицинскими организациями при оказании медицинской помощи с централизованными региональными и федеральными информационными ресурсами	НЕТ	ДА	НЕТ	НЕТ	ДА	Нарушение данного бизнес-процесса может привести к ошибочным управленческим решениям государственного органа власти.	Критичный
	– Обеспечение функционирования медицинского оборудования и информационных систем	Реализует функции: по обеспечению функционирования медицинских информационных систем администрированию медицинских информационных систем, проведению технического аудита доступа к базам данных медицинских информационных систем и контролю выполнения различных операций с информацией (сбор, предварительная обработка, консолидация, агрегация, накопление и хранение) инвентаризации и мониторинга состояния и состава технических средств и программного обеспечения медицинских информационных систем	ДА	НЕТ	ДА	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к причинению вреда жизни и здоровья людей	Критичный
	– Интеграция с медицинским	Реализует функцию	ДА	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	оборудованием	управление всеми данными, которые поступают из разных источников (анализаторы, проведенные вручную измерения, бумажные документы) и объединение этих данных в единую информационную базу данных клинико-диагностической лаборатории соединение практически с любыми автоматическими анализаторами и позволяет обмениваться информацией в режиме реального времени с любым АРМ, что дает мгновенный доступ к готовым результатам						может привести к причинению вреда жизни и здоровья людей	
	–								
	–								
	–								
Производственные	– Деятельность регистратуры и ведение медицинской карты лица которому оказывается медицинская помощь	Реализует функции: информационной поддержки процессов взаимодействия с пациентами, включая предоставление возможности записи и самозаписи пациента на прием к врачу, информационного наполнения личного кабинета пациента, выдачи пациенту электронных копий медицинских документов сбор и обработка сведений о лицах, которым оказывается медицинская помощь в том числе в электронной форме оказание государственных услуг в сфере здравоохранения в том числе в электронной	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не может привести к причинению ущерба жизни и здоровью людей, либо к прекращению или нарушению функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Некритичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
		форме							
	– Оказание медицинской помощи	Основной бизнес-процесс. Реализует функции: организация и оказание медицинской помощи, в рамках системы здравоохранения повышение качества оказания медицинской помощи разработки и осуществления мероприятий по профилактике возникновения и распространения заболеваний	ДА	НЕТ	ДА	НЕТ	ДА	Нарушение данного бизнес-процесса не может привести к причинению ущерба жизни и здоровью людей	Критичный
	–								
	–								
Финансово-экономические	– Обеспечение операционного учета	Реализует функции осуществления расчетов по основной деятельности организации сферы здравоохранения, вводу первичной информации, работе с банковскими документами	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не влияет на социальную, политическую, экономическую, экологическую, оборонную значимость.	Некритичный
	– Управление финансами организации сферы здравоохранения	Реализует функции по формированию и ведению бюджета организации сферы здравоохранения на очередной финансовый год и плановый период	НЕТ	НЕТ	ДА	НЕТ	НЕТ	Нарушение контрольной функции, реализуемой данным бизнес-процессом, может повлечь за собой ущерба субъекту критической информационной инфраструктуры, который является государственным унитарным предприятием	Критичный
	–								
	–								

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	–								
Иные	– образовательная деятельность	Предполагает организацию учебного процесса	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не влияет на социальную, политическую, экономическую, экологическую, оборонную значимость.	Некритичный
	– Юридическое сопровождение	Реализует функции: надлежащего правого регулирования деятельности организации сферы здравоохранения	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса не влияет на социальную, политическую, экономическую, экологическую, оборонную значимость.	Некритичный
	– мониторинг уровня защищенности информационных ресурсов организации сферы здравоохранения		ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к реализации компьютерных атак на информационные системы организации сферы здравоохранения и, как следствие к нарушению: – аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений государственным органом – управления или обеспечения работоспособности механизмов и устройств, нарушение функционирования которых может привести к последствиям, пагубно влияющим на жизнь и здоровье людей максимального времени отсутствия доступа в оказании государственных услуг	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	– формирование и проверка электронных подписей		ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к реализации компьютерных атак на информационные системы организации сферы здравоохранения и, как следствие к нарушению: – аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений государственным органом – управления или обеспечения работоспособности механизмов и устройств, нарушение функционирования которых может привести к последствиям, пагубно влияющим на жизнь и здоровье людей максимального времени отсутствия доступа в оказании государственных услуг	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	– обеспечение защиты врачебной тайны и персональных данных	Реализует функцию обеспечения исполнения требований законодательства РФ в области защиты информации и информационной безопасности	ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к реализации компьютерных атак на информационные системы организации сферы здравоохранения и, как следствие к нарушению: – аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений государственным органом – управления или обеспечения работоспособности механизмов и устройств, нарушение функционирования которых может привести к последствиям, пагубно влияющим на жизнь и здоровье людей максимального времени отсутствия доступа в оказании государственных услуг	Критичный

ОПИСАТЕЛЬНАЯ ЧАСТЬ РЕЕСТРА БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			ОЦЕНКА КРИТИЧНОСТИ БИЗНЕС-ПРОЦЕССОВ						
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРАТКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	КРИТЕРИИ ЗНАЧИМОСТИ					ОБОСНОВАНИЕ КРИТИЧНОСТИ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ
			Социальная	Политическая	Экономическая	Экологическая	Оборонная		
	– защита от вешних воздействий на информационные ресурсы		ДА	ДА	НЕТ	НЕТ	НЕТ	Нарушение данного бизнес-процесса может привести к реализации компьютерных атак на информационные системы организации сферы здравоохранения и, как следствие к нарушению: – аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений государственным органом – управления или обеспечения работоспособности механизмов и устройств, нарушение функционирования которых может привести к последствиям, пагубно влияющим на жизнь и здоровье людей максимального времени отсутствия доступа в оказании государственных услуг	Критичный

Приложение 8.

Справочные материалы по оценке критичности бизнес-процессов организации сферы здравоохранения

I. Критерии влияния бизнес-процессов организации сферы здравоохранения на показатели возможных последствий

№	ПОКАЗАТЕЛЬ ВОЗМОЖНЫХ ПОСЛЕДСТВИЙ (ПП-127)	КРИТЕРИЙ ВЛИЯНИЯ (ЗАДЕЙСТВОВАННОСТИ) БИЗНЕС-ПРОЦЕССА
I. Социальная значимость		
1	Причинение ущерба жизни и здоровью людей	Влияет, если бизнес-процесс задействован (обеспечивает) в управлении или обеспечении работоспособности механизмов и устройств, нарушение функционирования которых может привести: – к авариям, катастрофам с человеческими жертвами; – к бактериологическому, радиационному или химическому заражению; – к отключению приборов, обеспечивающих жизненно важные функции организма; – к нарушению технологий производства и хранения фармацевтической и медицинской продукции; – к иным последствиям, пагубно влияющим на жизнь и здоровье людей
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)
4	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)
5	Отсутствие доступа к государственной услуге	Влияет, если бизнес-процесс задействован: – в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры доступа к государственной услуге; – в аналитической, экспертной, учетной деятельности, необходимой для обеспечения функционирования органов власти и организаций сферы здравоохранения, оказывающих государственные услуги; – в обеспечении взаимодействия государственных органов власти, оказывающих государственные услуги
II. Политическая значимость		
6	Прекращение или нарушение функционирования государственного органа[76] в	Влияет, если бизнес-процесс задействован: – в аналитической, экспертной, учетной деятельности,

[76] В контексте настоящего документа под государственным органом подразумеваются федеральные органы государственной власти в сфере охраны здоровья, а также органы государственной власти субъектов Российской Федерации в сфере охраны здоровья

№	ПОКАЗАТЕЛЬ ВОЗМОЖНЫХ ПОСЛЕДСТВИЙ (ПП-127)	КРИТЕРИЙ ВЛИЯНИЯ (ЗАДЕЙСТВОВАННОСТИ) БИЗНЕС-ПРОЦЕССА
	части невыполнения возложенной на него функции (полномочия)	необходимой для принятия управленческих решений государственным органом; – в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры взаимодействия государственным органом; – в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры оповещения населения о чрезвычайных ситуациях; – в поддержании бесперебойного функционирования системы управления, необходимой для реализации возложенных на государственный орган полномочий
7	Нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ	
III. Экономическая значимость		
8	Возникновение ущерба субъекту КИИ[77]	Актуально только для организаций сферы здравоохранения, имеющих организационно-правовую форму «государственное унитарное предприятие» Влияет, если бизнес-процесс задействован: – в аналитической, экспертной, учетной деятельности, необходимой для принятия управленческих решений руководством государственного унитарного предприятия;
9	Возникновение ущерба бюджетам РФ, осуществляемых субъектом КИИ	Актуально только для организаций сферы здравоохранения, не применяющих нулевую ставку по налогу на прибыль и не оказывающих медицинских услуг, освобождаемых от налогообложения. Влияет, если бизнес-процесс задействован: – в обеспечении взаимодействия с организациями кредитно-финансовой сферы, включая страховые компании, биржи, банки, казначейство, налоговые органы
10	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций[78]	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)
IV. Экологическая значимость		
11	Вредные воздействия на окружающую среду	Актуально для организации сферы здравоохранения, использующих в своей деятельности источники ионизирующего излучения. (см. раздел «Ограничения и допущения»)
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка		
12	Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)

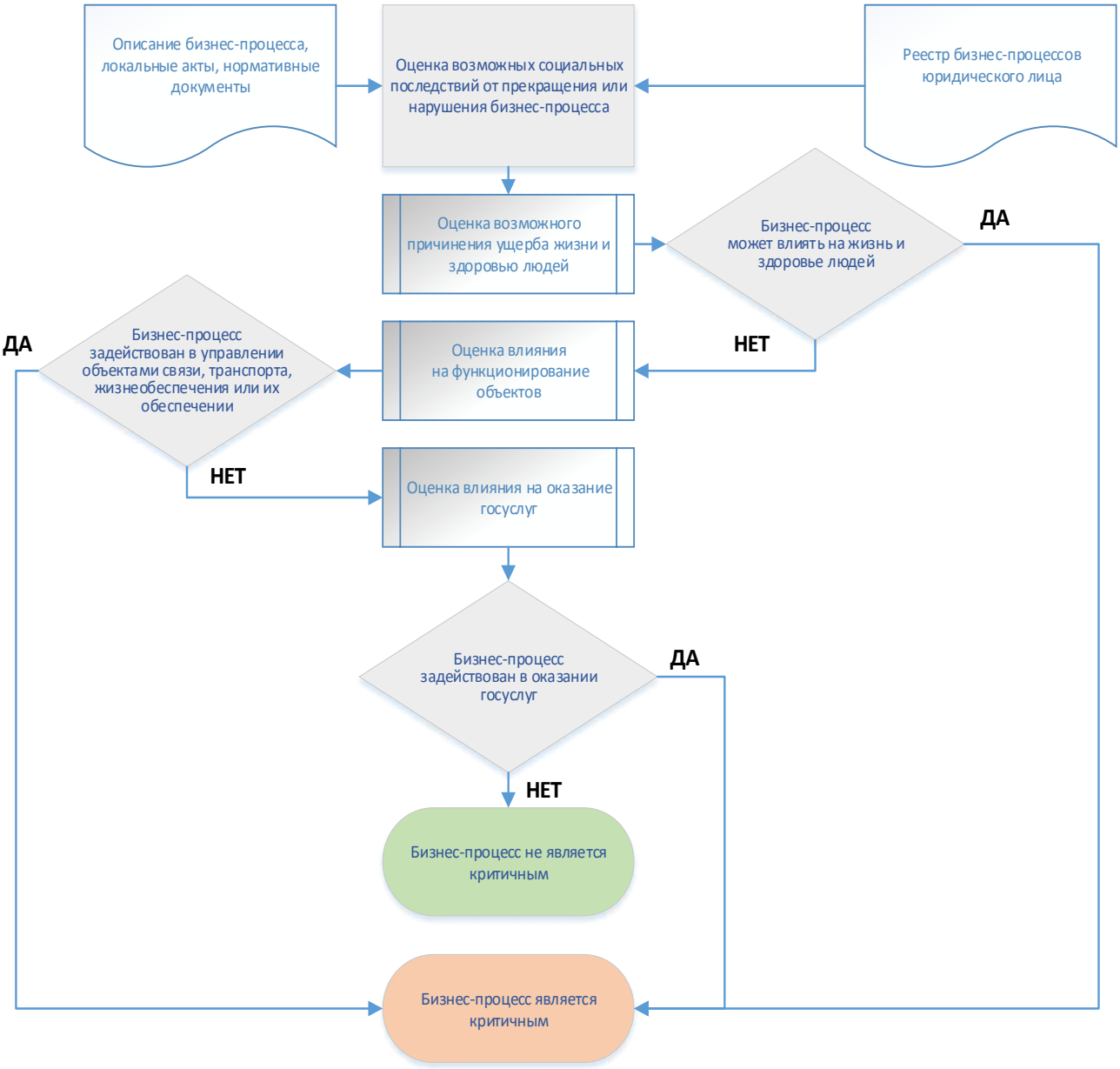
[77] Только для государственной корпорации, государственного унитарного предприятия, государственной компании, стратегического акционерного общества, стратегического предприятия

[78] Только для субъектов КИИ, являющихся в соответствии с законодательством РФ системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка

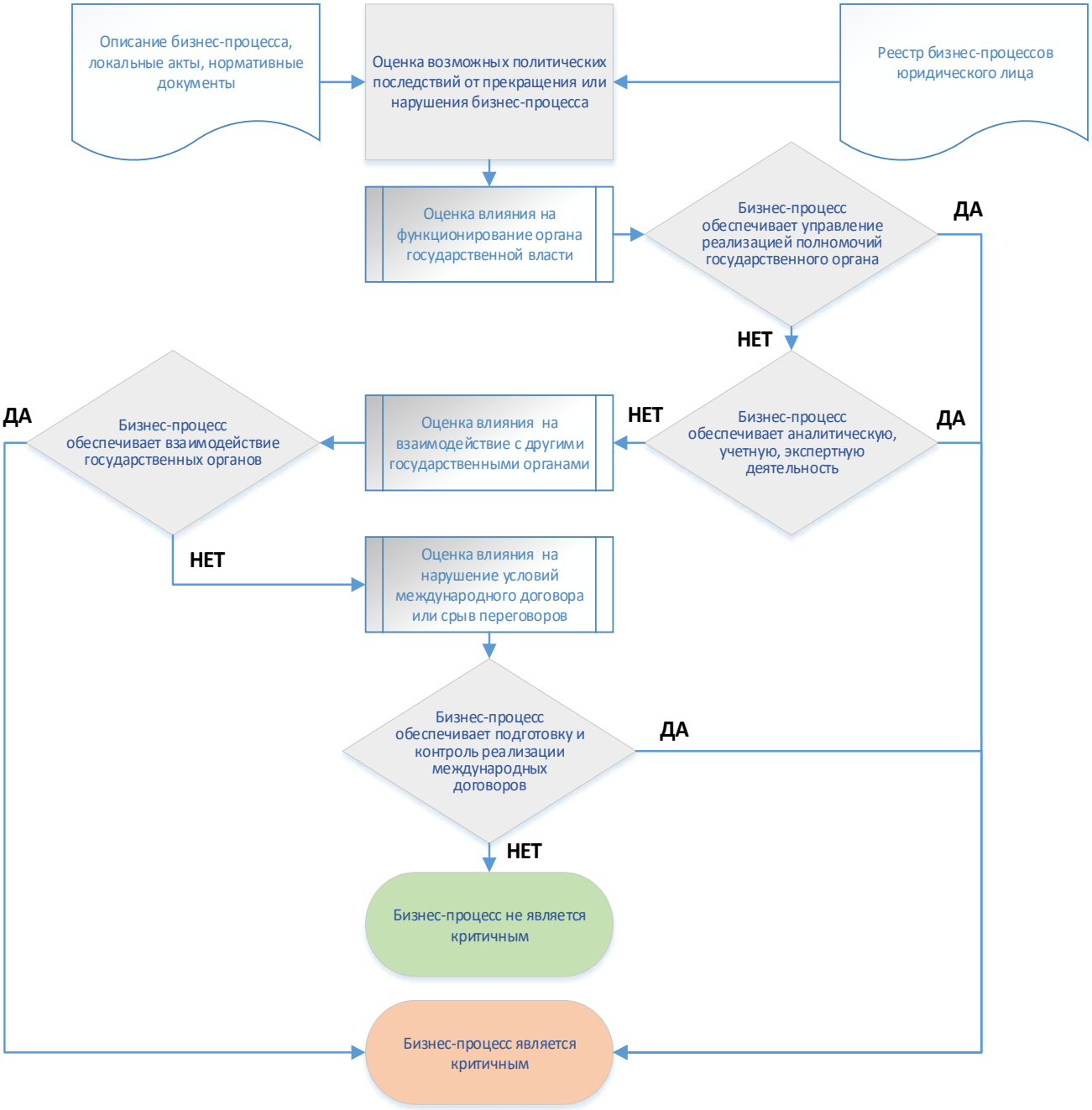
№	ПОКАЗАТЕЛЬ ВОЗМОЖНЫХ ПОСЛЕДСТВИЙ (ПП-127)	КРИТЕРИЙ ВЛИЯНИЯ (ЗАДЕЙСТВОВАННОСТИ) БИЗНЕС-ПРОЦЕССА
	управления (ситуационного центра)	
13	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)
14	Прекращение или нарушение функционирования (невыполнение установленных показателей) ИС в области обеспечения обороны страны, безопасности государства и правопорядка	Не оценивается. Не актуально для организации сферы здравоохранения (см. раздел «Ограничения и допущения»)

II. Алгоритмы оценки критичности бизнес-процессов

Алгоритм оценки социальной значимости бизнес-процесса



Алгоритм оценки политической значимости бизнес-процесса



Приложение 9.

Форма Перечня критичных бизнес-процессов организации сферы здравоохранения

Перечень критичных бизнес-процессов организации сферы здравоохранения

УТВЕРЖДАЮ

_____

(должность руководителя организации сферы здравоохранения)

_____

(Ф. И. О.)

« » _____ 20___ г.

ПЕРЕЧЕНЬ

критичных бизнес-процессов

<полное наименование организации сферы здравоохранения>

КРИТИЧНЫЕ БИЗНЕС-ПРОЦЕССЫ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			КОД ИС, АСУ, ИТКС, ЗАДЕЙСТВОВАННЫХ В РЕАЛИЗАЦИИ БИЗНЕС-ПРОЦЕССА И ОКАЗЫВАЮЩИХ ВЛИЯНИЕ								
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ	ИС-1	ИС-2	…	АСУ-1	АСУ-2	…	ИТКС-1	ИТКС-2	ПРИМЕЧАНИЕ
Управленческие	–										
	–										
Технологические	–										
	–										
Производственные	–										
	–										
Финансово-экономические	–										
	–										
Иные	–										

Председатель постоянно действующей Комиссии по категорированию объектов КИИ

<полное наименование организации сферы здравоохранения> _____

(Ф.И. О.)

«_____» _____ 202___ г.

Пример заполнения формы Перечня критичных бизнес-процессов организации сферы здравоохранения

КРИТИЧНЫЕ БИЗНЕС-ПРОЦЕССЫ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ			КОД ИС, АСУ, ИТКС, ЗАДЕЙСТВОВАННЫХ В РЕАЛИЗАЦИИ БИЗНЕС-ПРОЦЕССА И ОКАЗЫВАЮЩИХ ВЛИЯНИЕ								
КЛАСС БИЗНЕС-ПРОЦЕССОВ	БИЗНЕС-ПРОЦЕССЫ В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СФЕРЫ ЗДРАВООХРАНЕНИЯ	ЗАКЛЮЧЕНИЕ О КРИТИЧНОСТИ	ИС-1	ИС-2	…	АСУ-1	АСУ-2	…	ИТКС-1	ИТКС-2	ПРИМЕЧАНИЕ
Управленческие	– экспертно-аналитическая деятельность	Критичный									
	– централизованное диспетчерское управление	Критичный									
Технологические	– эксплуатация информационно-вычислительной системы	Критичный									
	– организация оптимального использования инфраструктуры	Критичный									
Производственные	– создание и сопровождение информационных ресурсов	Критичный									
Финансово-экономические	– планирование поставок комплектующих для производства	Критичный									
Иные	– обеспечение охраны объектов	Критичный									

Приложение 10.

Форма Реестра ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения

Форма Реестра ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения

УТВЕРЖДАЮ

_____

(должность руководителя организации сферы здравоохранения)

_____

(Ф.И. О.)

« » _____ 20__ г.

РЕЕСТР
информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, имеющихся на праве собственности, аренды или на ином законном основании в

_____

<полное наименование организации сферы здравоохранения>

КОД[79]	ТИП ОБЪЕКТА[80]	НАИМЕНОВАНИЕ	НАЗНАЧЕНИЕ	СФЕРА ДЕЯТЕЛЬНОСТИ[81]	ОСНОВАНИЕ[82]

Председатель постоянно действующей Комиссии
по категорированию объектов КИИ
<полное наименование организации сферы здравоохранения>

_____

(Ф.И. О.)

« » _____ 201__ г.

[79] Код вводится для удобства дальнейшего заполнения форм и устанавливается в произвольной форме, удобной для восприятия (например, ИС-1, ИС-2, … АСУ-1, АСУ-2, … ИТКС-1, ИТКС-2, …)

[80] Указывается один из следующих типов объекта: информационная система (ИС), автоматизированная система управления (АСУ), информационно-телекоммуникационная сеть (ИТКС).

[81] Указывается: здравоохранение (ЗО).

[82] Указываются реквизиты документа, подтверждающего право собственности, аренды или иное законное основание владения объектом

Образец заполнения Реестра ИС, ИТКС, АСУ, имеющихся в организации сферы здравоохранения

РЕЕСТР
информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, имеющихся на праве собственности, аренды или на ином законном основании в

_____

<полное наименование организации сферы здравоохранения>

КОД	ТИП ОБЪЕКТА	НАИМЕНОВАНИЕ	НАЗНАЧЕНИЕ	СФЕРА ДЕЯТЕЛЬНОСТИ	ОСНОВАНИЕ
ИС-2	ИС	Медицинская информационная система «*наименование*»	а) информационная поддержка принятия управленческих решений; б) мониторинг и управление потоками пациентов (электронная регистратура); в) ведение электронной медицинской карты пациента; г) оказание медицинской помощи с применением телемедицинских технологий; д) организация профилактики заболеваний, включая проведение диспансеризации, профилактических медицинских осмотров; е) организация иммунопрофилактики инфекционных болезней.	Здравоохранение	Приказ № 111 от 01.01.2020.

Председатель постоянно действующей Комиссии
по категорированию объектов КИИ
<полное наименование организации сферы здравоохранения>

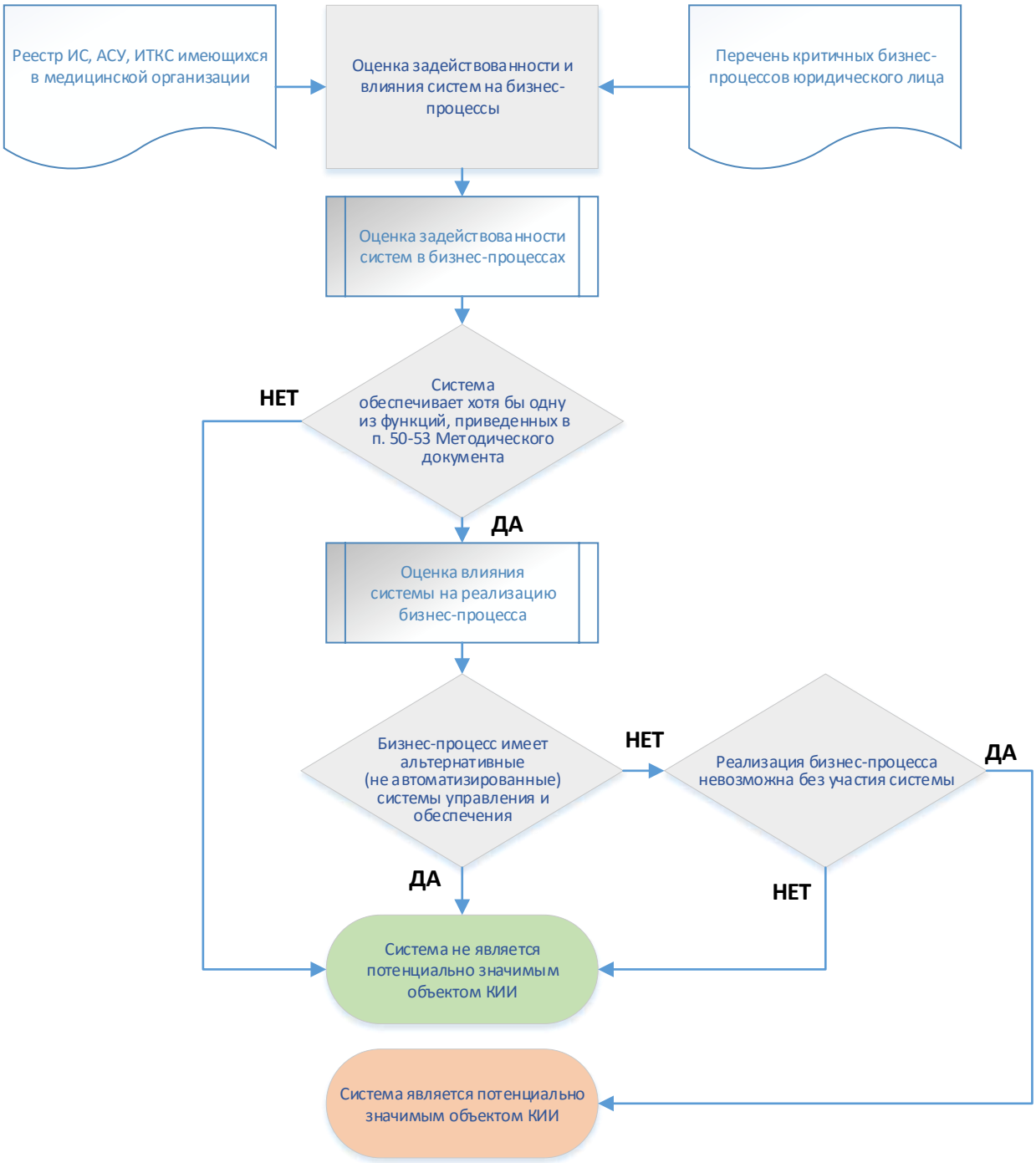
_____

(Ф.И. О.)

« » _____ 20____ г.

Приложение 11.

Алгоритм оценки задействованности и влияния ИС, ИТКС, АСУ на бизнес-процессы организации сферы здравоохранения



Приложение 12.

Форма Перечня объектов КИИ организации сферы здравоохранения, подлежащих категорированию

УТВЕРЖДАЮ

_____

Должность руководителя организации сферы здравоохранения или уполномоченного им лица

_____

Фамилия, имя, отчество (при наличии)

« __ » _____ 20__ г.

ПЕРЕЧЕНЬ
объектов критической информационной инфраструктуры

_____ ,

<полное наименование организации сферы здравоохранения>

подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[83]	Сфера (область) деятельности, в которой функционирует объект [84]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[85]
1.					
2.					
…					

[83] Указывается один из следующих типов объекта: ИС, ИТКС, АСУ.

[84] Указывается: здравоохранение.

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

n.					

Приложение 13.

Состав возможных событий (инцидентов), которые могут возникнуть в результате реализации наихудшего сценария целенаправленных компьютерных атак на ИС, ИТКС, АСУ

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[86])					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ						
Причинение ущерба жизни и здоровью людей (человек)	ДА			ДА	ДА	
Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	ДА			ДА	ДА	
Прекращение или нарушение функционирования объектов транспортной инфраструктуры	ДА			ДА	ДА	
Прекращение или нарушение функционирования сети связи	ДА			ДА	ДА	
Отсутствие доступа к государственной услуге	ДА			ДА	ДА	
ПОЛИТИЧЕСКАЯ ЗНАЧИМОСТЬ						
Прекращение или нарушение функционирования государственного органа	ДА			ДА	ДА	ДА
Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации		ДА	ДА	ДА	ДА	
ЭКОНОМИЧЕСКАЯ ЗНАЧИМОСТЬ						
Возникновение ущерба субъекту критической информационной инфраструктуры[87]	ДА	ДА	ДА	ДА	ДА	ДА
Возникновение ущерба бюджетам Российской Федерации				ДА		ДА

[86] Наихудший сценарий, учитывающий проведение целенаправленных компьютерных атак на объекты КИИ

[87] Для государственных корпораций, унитарных предприятий и компаний, стратегических акционерных обществ и предприятий

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[86])					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций[88]	ДА	ДА	ДА	ДА	ДА	
ЭКОЛОГИЧЕСКАЯ ЗНАЧИМОСТЬ						
Вредные воздействия на окружающую среду				ДА	ДА	
ЗНАЧИМОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ОБОРОНЫ СТРАНЫ, БЕЗОПАСНОСТИ ГОСУДАРСТВА И ПРАВОПОРЯДКА						
Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра)	ДА			ДА	ДА	ДА
Снижение показателей государственного оборонного заказа				ДА	ДА	ДА
Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	ДА			ДА	ДА	ДА

[88] Для системно значимой кредитной организации, оператора услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организации финансового рынка

Приложение 14.

Варианты обоснования неприменимости критериев значимости, установленных постановлением Правительства РФ от 08.02.2018 г. № 127

(Справочно)

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ	
Причинение ущерба жизни и здоровью людей	Организация сферы здравоохранения не относится к опасным производственным объектам в соответствии с законодательством Российской Федерации или к объектам транспортной инфраструктуры или не имеет в своем составе подразделения транспортной инфраструктуры.
	Организация сферы здравоохранения не относится к организациям, осуществляющим оказание медицинской помощи, проведение медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий, трансплантации (пересадки) органов и (или) тканей, обращения донорской крови и (или) ее компонентов в медицинских целях или имеет в своем составе подразделения по оказанию медицинской помощи.
	Организация сферы здравоохранения относится к опасным производственным объектам в соответствии с законодательством Российской Федерации или к объектам транспортной инфраструктуры или имеет в своем составе подразделения транспортной инфраструктуры, однако информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах юридического лица, не участвуют в обработке информации, необходимой для управления, контроля или мониторинга опасными производственными объектами или объектами транспортной инфраструктуры.
	Организация сферы здравоохранения относится к организациям, осуществляющим оказание медицинской помощи, проведение медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий, трансплантации (пересадки) органов и (или) тканей, обращения донорской крови и (или) ее компонентов в медицинских целях, однако информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах юридического лица, не участвуют в обработке информации, необходимой для оказания медицинской помощи, проведения медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических)

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
	мероприятий, трансплантации (пересадки) органов и (или) тканей, обращения донорской крови и (или) ее компонентов в медицинских целях и не осуществляют управление, контроль или мониторинг данных бизнес-процессов.
Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Организация сферы здравоохранения не относится к объектам водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения населения.
	Организация сферы здравоохранения относится к объектам водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения населения, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг объектами водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения населения.
	Организация сферы здравоохранения относится к объектам водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения населения, однако информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах организации сферы здравоохранения, не участвуют в обработке информации, необходимой для водоснабжения, канализации, электроснабжения, газоснабжения, теплоснабжения населения и не осуществляют управление, контроль или мониторинг данных бизнес-процессов.
Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Организация сферы здравоохранения не относится объектам транспортной инфраструктуры и не имеет в своем составе подразделения транспортной инфраструктуры.
	Организация сферы здравоохранения относится объектам транспортной инфраструктуры или имеет в своем составе подразделения транспортной инфраструктуры, однако, информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах организации сферы здравоохранения, не участвуют в обработке информации, необходимой для обеспечения транспортного сообщения или предоставления транспортных услуг и (или) управления, контроля или мониторинг транспортным сообщением или предоставлением транспортных услуг.
Прекращение или нарушение функционирования сети связи	Организация сферы здравоохранения не является оператором связи.
	Организация сферы здравоохранения является оператором связи, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг систем и элементов сети связи, необходимых для оказания услуг связи.
	Организация сферы здравоохранения является оператором связи, при этом, нарушение функционирования информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, может привести к нарушению или прекращению критичного бизнес-процесса, но не влечет за собой нарушение и (или) прекращение функционирования сети связи.
Отсутствие доступа к	Организация сферы здравоохранения не является государственным органом власти, оказывающим государственные услуги или

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
государственной услуге	юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, задействованной в процессе оказания государственной услуги.
	Организация сферы здравоохранения является государственным органом власти, оказывающим государственные услуги или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, задействованной в процессе оказания государственной услуги, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, задействованной в процессе оказания государственной услуги.
	Организация сферы здравоохранения является государственным органом власти, оказывающим государственные услуги, или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, задействованной в процессе оказания государственной услуги, однако, нарушение функционирования информационной системы, автоматизированной системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения не участвующей в обработке информации, необходимой для оказания государственной услуги, не влечет за собой нарушение и (или) прекращение доступа к государственной услуге.
ПОЛИТИЧЕСКАЯ ЗНАЧИМОСТЬ	
Прекращение или нарушение функционирования государственного органа	Организация сферы здравоохранения не является государственным органом власти или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в процессе выполнения возложенной на государственный орган власти функции (полномочия).
	Организация сферы здравоохранения является государственным органом власти или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в процессе выполнения возложенной на государственный орган власти функции (полномочия).
Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации	Организация сферы здравоохранения не является государственным органом власти или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в процессе подготовки условий планируемого к заключению международного договора Российской Федерации или контроля и мониторинга условий международного договора Российской Федерации.
	Организация сферы здравоохранения является государственным органом власти или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационной системы,

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
	автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в процессе подготовки условий планируемого к заключению международного договора Российской Федерации или контроля и мониторинга условий международного договора Российской Федерации.
	Организация сферы здравоохранения является государственным органом власти или юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, при этом, нарушение функционирования информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, имеющейся у организации сферы здравоохранения, не участвующей в обработке информации, необходимой для подготовки условий планируемого к заключению международного договора Российской Федерации или контроля и мониторинга условий международного договора Российской Федерации, не влечет за собой нарушение условий международного договора Российской Федерации.
ЭКОНОМИЧЕСКАЯ ЗНАЧИМОСТЬ	
Возникновение ущерба субъекту критической информационной инфраструктуры[89]	Организация сферы здравоохранения не является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием.
Возникновение ущерба бюджетам Российской Федерации	Организация сферы здравоохранения не является организацией, на которую в соответствии с Налоговым Кодексом Российской Федерации возложена обязанность уплачивать соответственно налоги, сборы, страховые взносы.
Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета	Организация сферы здравоохранения не осуществляет операций по банковским счетам и (или) без открытия банковского счета и не является системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка.
	Организация сферы здравоохранения осуществляет операции по банковским счетам и (или) без открытия банковского счета или является системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка, однако, критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в процессе проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций.

[89] Для государственных корпораций, государственных унитарных предприятий, государственных компаний, стратегических акционерных обществ, стратегических предприятий

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
	Организация сферы здравоохранения осуществляет операции по банковским счетам и (или) без открытия банковского счета или является системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка, однако информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах юридического лица, не участвуют в обработке информации, необходимой для проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций.
ЭКОЛОГИЧЕСКАЯ ЗНАЧИМОСТЬ	
Вредные воздействия на окружающую среду	Организация сферы здравоохранения не относится к опасным производственным объектам в соответствии с законодательством Российской Федерации или к объектам транспортной инфраструктуры или не имеет в своем составе подразделения транспортной инфраструктуры.
	Организация сферы здравоохранения относится к опасным производственным объектам в соответствии с законодательством Российской Федерации или к объектам транспортной инфраструктуры или имеет в своем составе подразделения транспортной инфраструктуры, однако информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах юридического лица не участвуют в обработке информации, необходимой для управления, контроля или мониторинга опасными производственными объектами или объектами транспортной инфраструктуры.
ЗНАЧИМОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ОБОРОНЫ СТРАНЫ, БЕЗОПАСНОСТИ ГОСУДАРСТВА И ПРАВОПОРЯДКА	
Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра)	Организация сферы здравоохранения не выполняет функции пункта управления (ситуационного центра) государственного органа власти, государственной корпорации или является юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в функционировании пункта управления (ситуационного центра) государственного органа власти, государственной корпорации.
	Организация сферы здравоохранения выполняет функции пункта управления (ситуационного центра) государственного органа власти, государственной корпорации или является юридическим лицом, обеспечивающим эксплуатацию информационной системы, автоматизированной системы управления, информационно-телекоммуникационной сети, задействованной в функционировании пункта управления (ситуационного центра) государственного органа власти, государственной корпорации, однако, критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, задействованных в функционировании пункта управления (ситуационного центра) государственного органа власти, государственной корпорации.
Снижение показателей	Организация сферы здравоохранения не осуществляет производство продукции (работ, услуг) в рамках государственного оборонного

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ОСНОВАНИЯ НЕПРИМЕНИМОСТИ КРИТЕРИЕВ ЗНАЧИМОСТИ, УСТАНОВЛЕННЫХ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РФ ОТ 08.02.2018 г. № 127 ДЛЯ ОЦЕНКИ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
государственного оборонного заказа	заказа
	Организация сферы здравоохранения осуществляет производство продукции (работ, услуг) в рамках государственного оборонного заказа, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, задействованных в производство продукции (работ, услуг) в рамках государственного оборонного заказа
	Организация сферы здравоохранения осуществляет производство продукции (работ, услуг) в рамках государственного оборонного заказа, однако, информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, имеющиеся у организации сферы здравоохранения, задействованные в критичных бизнес-процессах юридического лица не участвуют в обработке информации, необходимой для управления, контроля или мониторинга производства продукции (работ, услуг) в рамках государственного оборонного заказа
Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	Организация сферы здравоохранения не имеет информационных систем, функционирующих в области обеспечения обороны страны, безопасности государства и правопорядка
	Организация сферы здравоохранения не имеет информационных систем, функционирующих в области обеспечения обороны страны, безопасности государства и правопорядка, однако критичные бизнес-процессы организации сферы здравоохранения не осуществляют управление, контроль или мониторинг информационных систем, функционирующих в области обеспечения обороны страны, безопасности государства и правопорядка

Приложение 15.

Форма Протокола расчетов значений критериев значимости объектов КИИ организации сферы здравоохранения

УТВЕРЖДАЮ
Председатель постоянно действующей Комиссии
по категорированию объектов КИИ
<полное наименование организации сферы здравоохранения>

_____
(Ф.И. О.)
« » _____ 20___ г.

ПРОТОКОЛ №_____
расчетов значений критериев значимости объектов критической инфраструктуры

« » _____ 20__ г гор. _____

Председательствующий: _____

Секретарь: _____

Присутствовали: _____

_____

_____

Приглашенные эксперты: _____

_____

_____

Повестка дня:

1. Рассмотрение и утверждение расчетов значений критериев значимости объектов КИИ *<полное наименование организации сферы здравоохранения>*
2. Формирование Заключения о присвоении объекту КИИ *<полное наименование организации сферы здравоохранения>* или отсутствии необходимости присвоения одной из категорий значимости объектов КИИ.

Кворум для проведения заседания Комиссии по категорированию в соответствии с пунктом 7.4. Положения о постоянно действующей комиссии по категорированию объектов КИИ*<полное наименование организации сферы здравоохранения>* имеется.

В результате анализа представленных в Комиссию материалов, установлено:

I. СВЕДЕНИЯ ОБ ОБЪЕКТЕ КИИ[90]	
КОД ОБЪЕКТА КИИ	
СФЕРА ДЕЯТЕЛЬНОСТИ	
ТИП ОБЪЕКТА КИИ	
НАИМЕНОВАНИЕ	
НАЗНАЧЕНИЕ	
АРХИТЕКТУРА[91]	

II. СВЕДЕНИЯ О ВЗАИМОДЕЙСТВИИ ОБЪЕКТА КИИ С ДРУГИМИ ОБЪЕКТАМИ	
КАТЕГОРИЯ СЕТИ ЭЛЕКТРОСВЯЗИ[92]	
НАИМЕНОВАНИЕ ОПЕРАТОРА СВЯЗИ	
ЦЕЛЬ ВЗАИМОДЕЙСТВИЯ[93]	
СПОСОБ ВЗАИМОДЕЙСТВИЯ[94]	
ЗАВИСИМЫЙ ОБЪЕКТ КИИ[95]	
ТИП ЗАВИСИМОГО ОБЪЕКТА КИИ	

III. СВЕДЕНИЯ О КРИТИЧНЫХ БИЗНЕС-ПРОЦЕССАХ, В КОТОРЫХ ЗАДЕЙСТВОВАН ОБЪЕКТ КИИ[96]	
ТИП БИЗНЕС-ПРОЦЕССА	**НАИМЕНОВАНИЕ БИЗНЕС-ПРОЦЕССА**

[90] Заполняется в соответствии с Реестром информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, имеющихся на праве собственности, аренды или на ином законном основании

[91] Указывается: одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура

[92] Указывается: сеть общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи или сведения об отсутствии взаимодействия объекта КИИ с сетями электросвязи

[93] Указывается: передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель

[94] Указывается: проводной, беспроводной, технологии доступа, протоколы взаимодействия

[95] Указывается от какого другого объекта КИИ зависит функционирование оцениваемого объекта КИИ или сведения об отсутствии зависимости

[96] Указывается в соответствии с Реестром бизнес-процессов юридического лица

IV. РЕЗУЛЬТАТЫ РАСЧЕТА ЗНАЧЕНИЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТА КИИ[97]

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[98])					
	ОТКАЗ В ОБСЛУЖИВАНИИ	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	УТЕЧКА ДАННЫХ	МОДИФИКАЦИЯ (ПОДМЕНА) ДАННЫХ	НАРУШЕНИЕ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ	НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ
СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ						
Причинение ущерба жизни и здоровью людей		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к причинению ущерба жизни и здоровью людей	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к причинению ущерба жизни и здоровью людей			ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к причинению ущерба жизни и здоровью людей
Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению или нарушению функционирования объектов обеспечения жизнедеятельности населения	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к прекращению или нарушению функционирования объектов обеспечения жизнедеятельности населения	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к прекращению или нарушению функционирования объектов обеспечения жизнедеятельности населения
Прекращение или нарушение функционирования объектов транспортной инфраструктуры	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению или нарушению функционирования объектов транспортной инфраструктуры	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к прекращению или нарушению функционирования объектов транспортной инфраструктуры	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методический документ. Рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к прекращению или нарушению функционирования объектов транспортной инфраструктуры

[97] В данный раздел включено обоснование неприменимости критериев значимости с учетом раздела «Допущения и ограничения» и Приложений 13 и 14 настоящего документа
[98] Компьютерная атака по своей сути является одной из реализаций угроз безопасности информации

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[98])					
	ОТКАЗ В ОБСЛУЖИВАНИИ	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	УТЕЧКА ДАННЫХ	МОДИФИКАЦИЯ (ПОДМЕНА) ДАННЫХ	НАРУШЕНИЕ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ	НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ
Прекращение или нарушение функционирования сети связи	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению или нарушению функционирования сети связи	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к прекращению или нарушению функционирования сети связи	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 21)		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к прекращению или нарушению функционирования сети связи
Отсутствие доступа к государственной услуге		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению доступа к государственной услуге	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к прекращению доступа к государственной услуге	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Модификация (подмена) данных не может привести к прекращению доступа к государственной услуге		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к прекращению доступа к государственной услуге
ПОЛИТИЧЕСКАЯ ЗНАЧИМОСТЬ						
Прекращение или нарушение функционирования государственного органа		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению или нарушению функционирования государственного органа	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как утечка данных не может привести к прекращению или нарушению функционирования государственного органа			
Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Отказ в обслуживании не может привести к нарушению условий международного договора, срыву переговоров					ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к нарушению условий международного

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[98])					
	ОТКАЗ В ОБСЛУЖИВАНИИ	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	УТЕЧКА ДАННЫХ	МОДИФИКАЦИЯ (ПОДМЕНА) ДАННЫХ	НАРУШЕНИЕ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ	НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ
международного договора Российской Федерации	или подписания планируемого к заключению международного договора					договора, срыву переговоров или подписания планируемого к заключению международного договора
ЭКОНОМИЧЕСКАЯ ЗНАЧИМОСТЬ						
Возникновение ущерба субъекту критической информационной инфраструктуры[99]						
Возникновение ущерба бюджетам Российской Федерации	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Отказ в обслуживании не может причинить ущерб бюджетам Российской Федерации	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может причинить ущерб бюджетам Российской Федерации	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может причинить ущерб бюджетам Российской Федерации		ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Нарушение работы технических средств не может причинить ущерб бюджетам Российской Федерации	

[99] Для государственных корпораций, государственных унитарных предприятий, государственных компаний, стратегических акционерных обществ, стратегических предприятий

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[98])					
	ОТКАЗ В ОБСЛУЖИВАНИИ	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	УТЕЧКА ДАННЫХ	МОДИФИКАЦИЯ (ПОДМЕНА) ДАННЫХ	НАРУШЕНИЕ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ	НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ
Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций[100]	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 25)					ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не может привести к Прекращению или нарушению проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций
ЭКОЛОГИЧЕСКАЯ ЗНАЧИМОСТЬ						
Вредные воздействия на окружающую среду	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Отказ в обслуживании не оказывает вредного воздействия на окружающую среду	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Несанкционированный доступ не оказывает воздействия на окружающую среду	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не оказывает воздействия на окружающую среду			ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное использование вычислительных ресурсов не оказывает вредные воздействия на окружающую среду
ЗНАЧИМОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ОБОРОНЫ СТРАНЫ, БЕЗОПАСНОСТИ ГОСУДАРСТВА И ПРАВОПОРЯДКА						
Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра)	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может стать причиной прекращения или нарушения функционирования (невыполнение установленных	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может стать причиной прекращения или нарушения функционирования (невыполнение	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 27)		

[100] Для системно значимой кредитной организации, оператора услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организации финансового рынка

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак[98])					
	ОТКАЗ В ОБСЛУЖИВАНИИ	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	УТЕЧКА ДАННЫХ	МОДИФИКАЦИЯ (ПОДМЕНА) ДАННЫХ	НАРУШЕНИЕ РАБОТЫ ТЕХНИЧЕСКИХ СРЕДСТВ	НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ
	здравоохранения п. 27)	показателей) пункта управления (ситуационного центра)	установленных показателей) пункта управления (ситуационного центра)			
Снижение показателей государственного оборонного заказа	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Отказ в обслуживании не может стать причиной снижения показателей государственного оборонного заказа	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Несанкционированный доступ не может стать причиной снижения показателей государственного оборонного заказа	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может стать причиной снижения показателей государственного оборонного заказа	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 27)		
Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 27)	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как несанкционированный доступ не может привести к прекращению или нарушению функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка данных не может привести к прекращению или нарушению функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗНАЧИМОСТИ ДЛЯ ОБЪЕКТОВ КИИ НЕ ПРОВОДИТСЯ (см. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения п. 27)		

V. ЗАКЛЮЧЕНИЕ КОМИССИИ

(ВАРИАНТ 1)

На основании проведенных расчетов показателей критериев значимости объектов критической инфраструктуры для <*наименование ИС, АСУ, ИТКС*> постоянно действующая Комиссия по категорированию объектов КИИ <*полное наименование организации сферы здравоохранения*> пришла к заключению, что <*наименование ИС, АСУ, ИТКС*> относится к _____ категории значимости объектов критической инфраструктуры Российской Федерации, установленных постановлением Правительства РФ от 08.02.2018 г. № 127.

(*ВАРИАНТ 2*)

Проведенные расчеты показывают, что для <*наименование ИС, АСУ, ИТКС*> показатели критериев значимости объектов критической инфраструктуры, ниже установленных постановлением Правительства РФ от 08.02.2018 г. № 127. Постоянно действующая Комиссия по категорированию объектов КИИ <*полное наименование организации сферы здравоохранения*> пришла к заключению, что для <*наименование ИС, АСУ, ИТКС*> отсутствует необходимость присвоения одной из категорий значимости объектов критической инфраструктуры Российской Федерации, установленных постановлением Правительства РФ от 08.02.2018 г. № 127.

СЕКРЕТАРЬ КОМИССИИ

_____ – _____
(ФИО) (*подпись*)

ЧЛЕНЫ КОМИССИИ:

_____ – _____
(ФИО) (*подпись*)

_____ – _____
(ФИО) (*подпись*)

_____ – _____
(ФИО) (*подпись*)

_____ – _____
(ФИО) (*подпись*)

Приложение 16.

Форма Акта категорирования объекта КИИ организации сферы здравоохранения

УТВЕРЖДАЮ

_____

Должность руководителя организации сферы здравоохранения (уполномоченного лица)

_____

Фамилия, имя, отчество (при наличии)

« __ » _____ 20__ г.

АКТ № _____

категорирования объектов критической информационной инфраструктуры

_____

<полное наименование организации сферы здравоохранения>

_____ « » _____ 20___ г.

(место составления акта)

Во исполнение приказа *<должность руководителя организации сферы здравоохранения>* № _____ от _____, постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры *<полное наименование организации сферы здравоохранения>*, руководствуясь статьей 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства РФ от 08.02.2018 № 127, на основании результатов расчета показателей критериев значимости объектов критической информационной инфраструктуры, изложенных в Протоколе **№ _____** расчетов значений критериев значимости объектов критической инфраструктуры, пришла к следующему заключению:

<наименование ИС, АСУ, ИТКС, подлежащей категорированию[101]>,

построенная по архитектуре *<архитектура ИС, АСУ, ИТКС[102]>*, находящаяся у *<наименование организации сферы здравоохранения>*, на основании*<основание права собственности, аренды или иного законного основания владения>*, расположенная по адресу *<адрес размещения объекта КИИ[103]>*, предназначенная для *<назначение ИС, АСУ, ИТКС>*, обрабатывает информацию, необходимую для обеспечения *<наименование всех критичных бизнес-процессов[104] в которых задействована ИС, АСУ, ИТКС* и *(или) осуществляет управление, контроль или мониторинг этих процессов>*, относится к значимым объектам критической инфраструктуры *<категория[105]>* категории[106].

Председатель комиссии

_____ – _____,
(ФИО) (*подпись*)

Секретарь комиссии:

_____ – _____
(ФИО) (*подпись*)

[101] Указывается в соответствии с Перечнем объектов КИИ медицинской организации, подлежащих категорированию
[102] Указывается: одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура
[103] Указывается адрес размещения объекта, в том числе адрес обособленных подразделений, филиалов, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)
[104] Указывается в соответствии с Перечнем критических бизнес-процессов медицинской организации
[105] Указывается в соответствии с Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства РФ от 08.02.2018 № 127
[106] Либо указывается, что отсутствует необходимость присвоения ему одной из таких категорий

Приложение 17.

Справочные материалы по подготовке документов для отправки в ФСТЭК России

I. Образец сопроводительного письма в ФСТЭК России о направлении Перечня объектов КИИ организации сферы здравоохранения, подлежащих категорированию

<на фирменном бланке организации сферы здравоохранения>

Экспедиция ФСТЭК России,
2-е управление ФСТЭК России
ул. Старая Басманная, д. 17, г. Москва, 105066

О направлении Перечня объектов КИИ *<полное наименование организации сферы здравоохранения>*, подлежащих категорированию

В соответствии с Информационным сообщением ФСТЭК России от 17 апреля 2020 года № 240/84/611 направляем Перечень объектов КИИ *<полное наименование организации сферы здравоохранения>*, подлежащих категорированию.

В случае возникновения вопросов или необходимости получить какие-либо разъяснения с нашей стороны, просим обращаться к *<ФИО, телефон, адрес эл. почты>*.

Приложение: 1. Перечень объектов КИИ *<полное наименование организации сферы здравоохранения>*, подлежащих категорированию на _ *<число прописью>* листах в 1 (одном) экз.

2. Электронная копия Перечень объектов КИИ *<полное наименование организации сферы здравоохранения>*, подлежащих категорированию *<формат *.odt, *.ods>* на носителе _____ в 1 (одном) экз.

Все приложения только в адрес.

Руководитель

_____ (ФИО) – _____ (*подпись*),

II. Образец сопроводительного письма в ФСТЭК России о присвоении объекту КИИ категории значимости

<на фирменном бланке организации сферы здравоохранения>

Экспедиция ФСТЭК России,
2-е управление ФСТЭК России
ул. Старая Басманная, д. 17, г. Москва, 105066

О направлении сведений о результатах присвоения объектам КИИ <*полное наименование организации сферы здравоохранения*> категорий значимости либо об отсутствии необходимости присвоения им таких категорий

Во исполнение требований пункта 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 8 февраля 2018 года № 127) и в соответствии с Информационным сообщением ФСТЭК России от 17 апреля 2020 года № 240/84/611 направляем Сведения о результатах присвоения объектам КИИ <*полное наименование организации сферы здравоохранения*>категорий значимости либо об отсутствии необходимости присвоения им таких категорий.

В случае возникновения вопросов или необходимости получить какие-либо разъяснения с нашей стороны, просим обращаться к <*ФИО, телефон, адрес эл. почты*>.

Приложение: 1. Сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий на ___ (число прописью) листах в 1 (одном) экз.

2. Электронная копия Сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий <*формат, *.ods*> на носителе _____ в 1 (одном) экз.

Все приложения только в адрес.

Руководитель

_____ – _____,
(ФИО) (*подпись*)

III. Форма Сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
1.4.	Назначение объекта	
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
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) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

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 и (или) провайдера хостинга	

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), 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)	
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

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

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных	

	средств) и их количество	
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 (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	

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	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости

8.1.	Категория значимости, которая присвоена объекту либо информация о не присвоении объекту ни одной из таких категорий	
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	

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	

_____ _____ _____

(Наименование должности руководителя организации сферы здравоохранения или уполномоченного им лица) *(подпись)* *(инициалы, фамилия)*

М.П.
(при наличии печати)

"__" _____ 20__ г.

IV. Классификация и характеристика сетей электросвязи

ТИП СЕТИ	ХАРАКТЕРИСТИКА СЕТИ (ОПИСАНИЕ)	ВЗАИМОСВЯЗЬ С ОРГАНИЗАЦИЯМ СФЕРЫ ЗДРАВООХРАНЕНИЯ
Сеть связи общего пользования	Комплекс взаимодействующих сетей электросвязи, определяемых географически в пределах обслуживаемой территории	Сети связи общего пользования могут быть задействованы во всех организациях сферы здравоохранения. Взаимодействие объекта КИИ и сетей электросвязи общего пользования определяется наличием в организации сферы здравоохранения договоров с организациями связи на предоставление услуг связи, в том числе телематических услуг, услуг связи по предоставлению каналов связи и передаче данных. Примером сети связи общего пользования является сеть Интернет.
Выделенные сети связи	Сети электросвязи для оказания услуг электросвязи ограниченному кругу пользователей или группам таких пользователей. Выделенные сети связи могут взаимодействовать между собой. Выделенные сети связи не имеют присоединения к сети связи общего пользования	Выделенные сети связи могут выполнять роль среды передачи данных внутри организации сферы здравоохранения. Примером выделенной сети связи является сеть Интранет.
Технологические сети связи	Сети связи для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве	Технологические сети связи, как правило, задействуются для обеспечения деятельности автоматизированных систем диагностики заболеваний и прогнозирования результатов их лечения и медицинских комплексов программно-аппаратных. Технологические сети связи могут взаимодействовать между собой посредством подключения к сетям связи общего пользования.
Сети связи специального назначения	Сети связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка. Сети связи специального назначения могут быть присоединены к сети связи общего пользования	Сети связи специального назначения как правило используются органами управления системой здравоохранения. Примером сети связи специального назначения является система межведомственного электронного взаимодействия (СМЭВ-3).

V. Взаимосвязь возможных угроз безопасности информации и инцидентов

ВОЗМОЖНЫЕ УГРОЗЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак)					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	НЕТ
Угрозы доступа (проникновения) в операционную среду	НЕТ	ДА	ДА	ДА	НЕТ	НЕТ
Угрозы удаленного доступа (сетевые атаки)	ДА	ДА	ДА	ДА	ДА	ДА
Угрозы программно-математического воздействия (вирусные атаки)	НЕТ	ДА	ДА	ДА	НЕТ	ДА
Угрозы социально-психологического характера	ДА	ДА	ДА	ДА	ДА	ДА

VI. Взаимосвязь возможных угроз безопасности информации и объектов воздействия ИС, ИТКС, АСУ

ВОЗМОЖНЫЕ УГРОЗЫ	ОБЪЕКТЫ ВОЗДЕЙСТВИЯ													ХАРАКТЕРИСТИКА УГРОЗЫ
	Оборудование ИС, ИТКС, АСУ	Пользователи ИС, ИТКС, АСУ	Обеспечивающий персонал	Центр обработки данных	Серверное оборудование	Телекоммуникационное оборудование	Исполнительные устройства	Сетевое оборудование	Технологическое оборудование	Программные компоненты для передачи данных по сетям	Файлы данных (информация)	Базы данных с информацией	Прикладные программы доступа и обработки информации	
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	ДА	ДА	НЕТ	НЕТ	ДА	Преднамеренные изменения служебных данных, игнорирование предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажение (модификация) самих данных
Угрозы доступа (проникновения) в операционную среду	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	НЕТ	НЕТ	ДА	Несанкционированный доступ к информации или внедрение вредоносных программ путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия
Угрозы удаленного доступа (сетевые атаки)	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	ДА	ДА	ДА	Захват контроля (повышение прав) над удалённой ИС, ИТКС, АСУ, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, осуществляемое по каналам связи
Угрозы	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	НЕТ	ДА	НЕТ	ДА	ДА	ДА	ДА	Воздействие на ИС, ИТКС, АСУ с помощью

ВОЗМОЖНЫЕ УГРОЗЫ	ОБЪЕКТЫ ВОЗДЕЙСТВИЯ													ХАРАКТЕРИСТИКА УГРОЗЫ
	Оборудование ИС, ИТКС, АСУ	Пользователи ИС, ИТКС, АСУ	Обеспечивающий персонал	Центр обработки данных	Серверное оборудование	Телекоммуникационное оборудование	Исполнительные устройства	Сетевое оборудование	Технологическое оборудование	Программные компоненты для передачи данных по сетям	Файлы данных (информация)	Базы данных с информацией	Прикладные программы доступа и обработки информации	
программно-математического воздействия (вирусные атаки)														вредоносных программ для дестабилизации ИС, ИТКС, АСУ, либо отказа в обслуживании, а также получения данных пользователей
Угрозы социально-психологического характера	НЕТ	ДА	ДА	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Несанкционированный доступ к информации или внедрение вредоносных программ путем воздействия на физические, моральные, психологические особенности пользователей ИС, ИТКС, АСУ либо деструктивные действия пользователей ИС, АСУ, ИТКС на почве антагонистических отношений или неудовлетворенности своим положением

VII. Классификация, характеристика и возможности нарушителей по реализации угроз безопасности информации

ТИП НАРУШИТЕЛЯ	КЛАСС НАРУШИТЕЛЯ	ОПИСАНИЕ НАРУШИТЕЛЯ	УГРОЗЫ				
			создания нештатных режимов работы	доступа (проникновения) в операционную среду	удаленного доступа (сетевые атаки)	программно-математического воздействия (вирусные атаки)	социально-психологического характера
H_1	Внешний антропогенный	Нарушитель с базовым потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, не имеет доступа в зону эксплуатации ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки (хакер)	НЕТ	ДА	ДА	ДА	НЕТ
H_2	Внешний антропогенный	Нарушитель с базовым повышенным потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, не имеет доступа в зону эксплуатации ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, самостоятельно реализует компьютерные атаки (преступный элемент, хакерская группа)	НЕТ	ДА	ДА	ДА	ДА
H_3	Внутренний или внешний антропогенный	Нарушитель с базовым низким потенциалом, имеет физический доступ к средствам (системам) обработки ИС, ИТКС, АСУ организации сферы здравоохранения, но не имеет прав пользователя ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (обслуживающий персонал, поставщик)	ДА	НЕТ	НЕТ	ДА	НЕТ
H_4	Внутренний антропогенный	Нарушитель с базовым низким потенциалом, является пользователем, в том числе	НЕТ	ДА	ДА	ДА	НЕТ

ТИП НАРУШИТЕЛЯ	КЛАСС НАРУШИТЕЛЯ	ОПИСАНИЕ НАРУШИТЕЛЯ	УГРОЗЫ				
			создания нештатных режимов работы	доступа (проникновения) в операционную среду	удаленного доступа (сетевые атаки)	программно-математического воздействия (вирусные атаки)	социально-психологического характера
		удаленным, ИС, ИТКС, АСУ организации сферы здравоохранения, но не имеет прав администрирования и конфигурирования средств (систем) ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки (пользователь)					
H_5	Внутренний антропогенный	Нарушитель с базовым повышенным потенциалом является пользователем, в том числе удаленным, ИС, ИТКС, АСУ организации сферы здравоохранения, имеет права администрирования и конфигурирования средств (систем) ИС, ИТКС, АСУ, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (привилегированный пользователь)	ДА	ДА	ДА	ДА	НЕТ
H_6	Внешний антропогенный	Нарушитель с высоким потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа методов компьютерных атак (специальные службы иностранных государств)	ДА	ДА	ДА	ДА	ДА

VIII. Примеры определения угроз безопасности информации, нарушителей и последствий инцидентов для организации сферы здравоохранения

Пример 1. ГИС «Наименование»

1. На основании раздела IV Протокола расчетов значений критериев значимости для категорируемой ИС установлено, что для ГИС «Наименование» характерны два критерия значимости:

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак)					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ						
Отсутствие доступа к государственной услуге	ДА			ДА	ДА	
ПОЛИТИЧЕСКАЯ ЗНАЧИМОСТЬ						
Прекращение или нарушение функционирования государственного органа	ДА			ДА	ДА	ДА

В п. 7.1. Формы представления Сведений о категорировании вносится:

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	1. Инциденты, которые могут привести к отсутствию доступа к государственной услуге: – отказ в обслуживании; – модификация (подмена) данных – нарушение работы технических средств 2. Инциденты, которые могут привести к прекращению или нарушению функционирования государственного органа: – отказ в обслуживании; – модификация (подмена) данных – нарушение работы технических средств – незаконное использование вычислительных ресурсов

2. На основании определенных в п. 1 возможных событий (инцидентов)с учетом данных раздела V Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17) выявлены следующие угрозы безопасности информации для ГИС «Наименование»:

ВОЗМОЖНЫЕ УГРОЗЫ	**ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак)**					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	НЕТ
Угрозы доступа (проникновения) в операционную среду	НЕТ	ДА	ДА	ДА	НЕТ	НЕТ
Угрозы удаленного доступа (сетевые атаки)	ДА	ДА	ДА	ДА	ДА	ДА
Угрозы программно-математического воздействия (вирусные атаки)	НЕТ	ДА	ДА	ДА	НЕТ	ДА
Угрозы социально-психологического характера	ДА	ДА	ДА	ДА	ДА	ДА

Потенциальными угрозами безопасности информации для ГИС «Наименование» являются:

- угрозы создания нештатных режимов работы;
- угрозы доступа (проникновения) в операционную среду
- угрозы удаленного доступа (сетевые атаки)
- угрозы программно-математического воздействия (вирусные атаки)
- угрозы социально-психологического характера

3. При актуализации состава возможных угроз безопасности информации с учетом с учетом структурно-функциональных характеристик ГИС «Наименование» определены следующие объекты воздействия:
   - Оборудование ИС, ИТКС, АСУ
   - Пользователи ИС, ИТКС, АСУ
   - Обеспечивающий персонал
   - Центр обработки данных
   - Серверное оборудование
   - Сетевое оборудование
   - Программные компоненты для передачи данных по сетям
   - Файлы данных (информация)
   - Базы данных с информацией

– Прикладные программы доступа и обработки информации

Взаимосвязи возможных угроз безопасности информации и событий (инцидентов) безопасности (раздел V Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) показали, что состав угроз после актуализации не изменился.

ВОЗМОЖНЫЕ УГРОЗЫ	ОБЪЕКТЫ ВОЗДЕЙСТВИЯ													ХАРКАТЕРИСТИКА УГРОЗЫ
	Оборудование ИС, ИТКС, АСУ	Пользователи ИС, ИТКС, АСУ	Обеспечивающий персонал	Центр обработки данных	Серверное оборудование	Телекоммуникационное оборудование	Исполнительные устройства	Сетевое оборудование	Технологическое оборудование	Программные компоненты для передачи данных по сетям	Файлы данных (информация)	Базы данных с информацией	Прикладные программы доступа и обработки информации	
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	ДА	ДА	НЕТ	НЕТ	ДА	Преднамеренные изменения служебных данных, игнорирование предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажение (модификации) самих данных
Угрозы доступа (проникновения) в операционную среду	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	НЕТ	НЕТ	ДА	Выполнение несанкционированного доступа к информации или внедрения вредоносных программ путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия
Угрозы удаленного доступа (сетевые атаки)	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	ДА	ДА	ДА	Захват контроля (повышение прав) над удалённой ИС, ИТКС, АСУ, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, осуществляемое по каналам связи
Угрозы программно-математического воздействия (вирусные атаки)	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	НЕТ	ДА	НЕТ	ДА	ДА	ДА	ДА	Воздействие на ИС, ИТКС, АСУ с помощью вредоносных программ для дестабилизации ИС, ИТКС, АСУ, либо отказа в обслуживании, а также получения данных пользователей
Угрозы социально-психологического характера	НЕТ	ДА	ДА	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	Выполнение несанкционированного доступа к информации или внедрения вредоносных программ путем воздействия на физические, моральные, психологические особенности пользователей ИС, ИТКС, АСУ либо деструктивные действия пользователей ИС, АСУ, ИТКС на почве антагонистических отношений или неудовлетворенности своим положением

В п. 6.2 Формы представления Сведений о категорировании вносится:

6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	Угрозы, которые могут привести к отсутствию доступа к государственной услуге, а также к прекращению или нарушению функционирования государственного органа: – угрозы создания нештатных режимов работы; – угрозы доступа (проникновения) в операционную среду – угрозы удаленного доступа (сетевые атаки) – угрозы программно-математического воздействия (вирусные атаки) – угрозы социально-психологического характера

4. На основании полученного перечня актуальных угроз безопасности информации и возможностей нарушителей по реализации угроз безопасности информации (раздел VI Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) определены типы (категории) возможных нарушителей:

ТИП НАРУШИТЕЛЯ	КЛАСС НАРУШИТЕЛЯ	ОПИСАНИЕ НАРУШИТЕЛЯ	УГРОЗЫ				
			создания нештатных режимов работы	доступа (проникновения) в операционную среду	удаленного доступа (сетевые атаки)	программно-математического воздействия (вирусные атаки)	социально-психологического характера
H_1	Внешний антропогенный	Нарушители с базовым потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, не имеет доступа в зону эксплуатации ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки (хакер)	НЕТ	ДА	ДА	ДА	НЕТ
H_2	Внешний антропогенный	Нарушитель с базовым повышенным потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, не имеет доступа в зону эксплуатации ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, самостоятельно реализует компьютерные атаки (преступный элемент, хакерская группа)	НЕТ	ДА	ДА	ДА	ДА
H_3	Внутренний или внешний антропогенный	Нарушитель с базовым низким потенциалом, имеет физический доступ к средствам (системам) обработки ИС, ИТКС, АСУ организации сферы здравоохранения, но не имеет прав пользователя ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (обслуживающий персонал, поставщик)	ДА	НЕТ	НЕТ	ДА	НЕТ
H_4	Внутренний антропогенный	Нарушитель с базовым низким потенциалом, является пользователем, в том числе удаленным, ИС, ИТКС, АСУ организации сферы здравоохранения, но не имеет прав администрирования и конфигурирования средств (систем) ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки (пользователь)	НЕТ	ДА	ДА	ДА	НЕТ
H_5	Внутренний антропогенный	Нарушитель с базовым повышенным потенциалом является пользователем, в том числе удаленным, ИС, ИТКС, АСУ организации сферы здравоохранения, имеет права администрирования и конфигурирования средств (систем) ИС, ИТКС, АСУ, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (привилегированный пользователь)	ДА	ДА	ДА	ДА	НЕТ
H_6	Внешний антропогенный	Нарушитель с высоким потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа методов	ДА	ДА	ДА	ДА	ДА

ТИП НАРУШИТЕЛЯ	КЛАСС НАРУШИТЕЛЯ	ОПИСАНИЕ НАРУШИТЕЛЯ	УГРОЗЫ				
			создания нештатных режимов работы	доступа (проникновения) в операционную среду	удаленного доступа (сетевые атаки)	программно-математического воздействия (вирусные атаки)	социально-психологического характера
		компьютерных атак (специальные службы иностранных государств)					

В п. 6.1 Формы представления Сведений о категорировании вносится:

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	1. Внешний антропогенный H_1 (хакер) нарушитель с базовым потенциалом, не являющийся пользователем ГИС «Наименование», не имеющий доступа в зону эксплуатации ГИС «Наименование», самостоятельно осуществляющий создание методов и средств реализации компьютерных атак, а также самостоятельно реализующий компьютерные атаки 2. Внешний антропогенный H_2 (преступный элемент, хакерская группа) нарушитель с базовым повышенным потенциалом, не являющийся пользователем ГИС «Наименование», не имеющий доступа в зону эксплуатации ГИС «Наименование», самостоятельно осуществляющий создание методов и средств реализации компьютерных атак, самостоятельно реализующий компьютерные атаки 3. Внутренний или внешний антропогенный H_3 (обслуживающий персонал, поставщик) Нарушитель с базовым низким потенциалом, имеет физический доступ к средствам (системам) обработки ГИС «Наименование», но не имеет прав пользователя ГИС «Наименование», самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак 4. Внутренний антропогенный H_4 (пользователь) нарушитель с базовым низким потенциалом, является пользователем, в том числе удаленным, ГИС «Наименование», но не имеет прав

		администрирования и конфигурирования средств (систем) ГИС «Наименование», самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки 5. Внутренний антропогенный H_5 (привилегированный пользователь) нарушитель с базовым повышенным потенциалом является пользователем, в том числе удаленным, ГИС «Наименование», имеет права администрирования и конфигурирования средств (систем) ГИС «Наименование», осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак 6. Внешний антропогенный H_6 (специальные службы иностранных государств) нарушитель с высоким потенциалом, не является пользователем ГИС «Наименование», осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа методов компьютерных атак

Пример 2. МПКС

1. На основании раздела IV Протокола расчетов значений критериев значимости для категорируемой ИС установлено, что для МПКС (аппаратура для искусственной вентиляции легких) характерны следующие критерия значимости:

КРИТЕРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	**ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак)**					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ						
Причинение ущерба жизни и здоровью людей (человек)	ДА			ДА	ДА	

В п. 7.1. Формы представления Сведений о категорировании вносится:

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 данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления инцидентов	1. Инциденты, которые могут привести к ущербу жизни и здоровью людей: – отказ в обслуживании; – модификация (подмена) данных – нарушение работы технических средств

2. На основании определенных в п. 1 возможных событий (инцидентов) с учетом данных раздела V Справочных материалов по подготовке документов для отправки в ФСТЭК России (Приложение 17) выявлены следующие угрозы безопасности информации для МПКС:

ВОЗМОЖНЫЕ УГРОЗЫ	**ВОЗМОЖНЫЕ ИНЦИДЕНТЫ (результат компьютерных атак)**					
	отказ в обслуживании	несанкционированный доступ	утечка данных	модификация (подмена) данных	нарушение работы технических средств	незаконное использование вычислительных ресурсов
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	НЕТ
Угрозы доступа (проникновения) в операционную среду	НЕТ	ДА	ДА	ДА	НЕТ	НЕТ
Угрозы удаленного доступа (сетевые атаки)	ДА	ДА	ДА	ДА	ДА	ДА
Угрозы программно-математического воздействия (вирусные атаки)	НЕТ	ДА	ДА	ДА	НЕТ	ДА
Угрозы социально-психологического характера	ДА	ДА	ДА	ДА	ДА	ДА

3. Учитывая структурно-функциональные характеристики МПКС, включающие структуру и состав системы, физические, логические, функциональные и технологические взаимосвязи, исключающие возможность удаленного доступа, угрозы удаленного доступа не являются актуальными и исключаются.

ВОЗМОЖНЫЕ УГРОЗЫ	Исполнительные устройства	Прикладные программы доступа и обработки информации	ХАРАКТЕРИСТИКА УГРОЗЫ
Угрозы создания нештатных режимов работы	ДА	ДА	Преднамеренные изменения служебных данных, игнорирование предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажение (модификации) самих данных
Угрозы доступа (проникновения) в операционную среду	ДА	ДА	Выполнение несанкционированного доступа к информации или внедрения вредоносных программ путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия
Угрозы удаленного доступа (сетевые атаки)	ДА	ДА	Захват контроля (повышение прав) над удалённой ИС, ИТКС, АСУ, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, осуществляемое по каналам связи
Угрозы программно-математического воздействия (вирусные атаки)	НЕТ	ДА	Воздействие на ИС, ИТКС, АСУ с помощью вредоносных программ для дестабилизации ИС, ИТКС, АСУ, либо отказа в обслуживании, а также получения данных пользователей
Угрозы социально-психологического характера	НЕТ	НЕТ	Выполнение несанкционированного доступа к информации или внедрения вредоносных программ путем воздействия на физические, моральные, психологические особенности пользователей ИС, ИТКС, АСУ либо деструктивные действия пользователей ИС, АСУ, ИТКС на почве антагонистических отношений или неудовлетворенности своим положением

При актуализации состава возможных угроз безопасности информации с учетом с учетом структурно-функциональных характеристик МПКС определены следующие объекты воздействия:

- Исполнительные устройства
- Прикладные программы доступа и обработки информации

Взаимосвязи возможных угроз безопасности информации и событий (инцидентов) безопасности (раздел V Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) показал, что угрозы социально-психологического характера не являются актуальными.

В п. 6.2 Формы представления Сведений о категорировании вносится:

6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	Угрозы, которые могут привести к отсутствию доступа к ущербу жизни и здоровью людей: – угрозы создания нештатных режимов работы

4. На основании полученного перечня актуальных угроз безопасности информации и возможностей нарушителей по реализации угроз безопасности информации (раздел VI Справочных материалов по подготовке документов для отправки в ФСТЭК России, Приложение 17) определены типы (категории) возможных нарушителей:

ТИП НАРУШИТЕЛЯ	КЛАСС НАРУШИТЕЛЯ	ОПИСАНИЕ НАРУШИТЕЛЯ	создания нештатных режимов работы
H_3	Внутренний или внешний антропогенный	Нарушитель с базовым низким потенциалом, имеет физический доступ к средствам (системам) обработки ИС, ИТКС, АСУ организации сферы здравоохранения, но не имеет прав пользователя ИС, ИТКС, АСУ, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (обслуживающий персонал, поставщик)	ДА
H_5	Внутренний антропогенный	Нарушитель с базовым повышенным потенциалом является пользователем, в том числе удаленным, ИС, ИТКС, АСУ организации сферы здравоохранения, имеет права администрирования и конфигурирования средств (систем) ИС, ИТКС, АСУ, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак (привилегированный пользователь)	ДА
H_6	Внешний антропогенный	Нарушитель с высоким потенциалом, не является пользователем ИС, ИТКС, АСУ организации сферы здравоохранения, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа методов компьютерных атак (специальные службы иностранных государств)	ДА

Учитывая, что нарушители типа H_6 имеют мотивацию только в отношении определенной категории пациентов, данный тип нарушителей не актуален для обычного организации сферы здравоохранения и могут быть исключены из состава актуальных.

В п. 6.1 Формы представления Сведений о категорировании вносится:

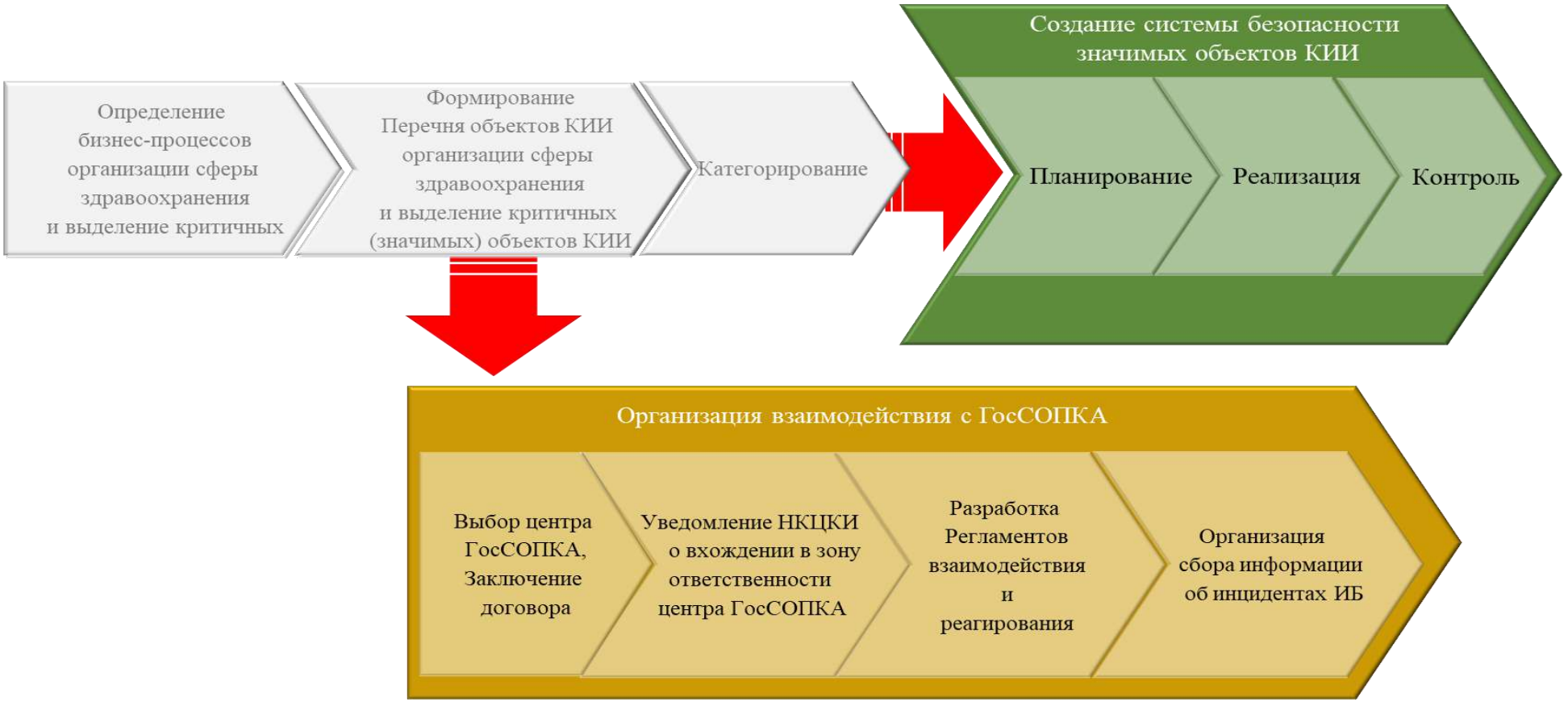
6.1.	Категория нарушителя (внешний или внутренний), краткая	1. Внутренний или внешний антропогенный H_3 (обслуживающий персонал, поставщик)

	характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Нарушитель с базовым низким потенциалом, имеет физический доступ к средствам (системам) обработки МПКС, но не имеет прав пользователя МПКС, самостоятельно осуществляет создание методов и средств реализации компьютерных атак, а также самостоятельно реализует компьютерные атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак 2. Внутренний антропогенный H_5 (привилегированный пользователь) нарушитель с базовым повышенным потенциалом является пользователем, в том числе удаленным, МПКС, имеет права администрирования и конфигурирования средств (систем) МПКС, осуществляет создание методов и средств реализации компьютерных атак, а также реализацию компьютерных атаки с привлечением отдельных специалистов, имеющих опыт в разработке и анализе методов компьютерных атак

Приложение 18.

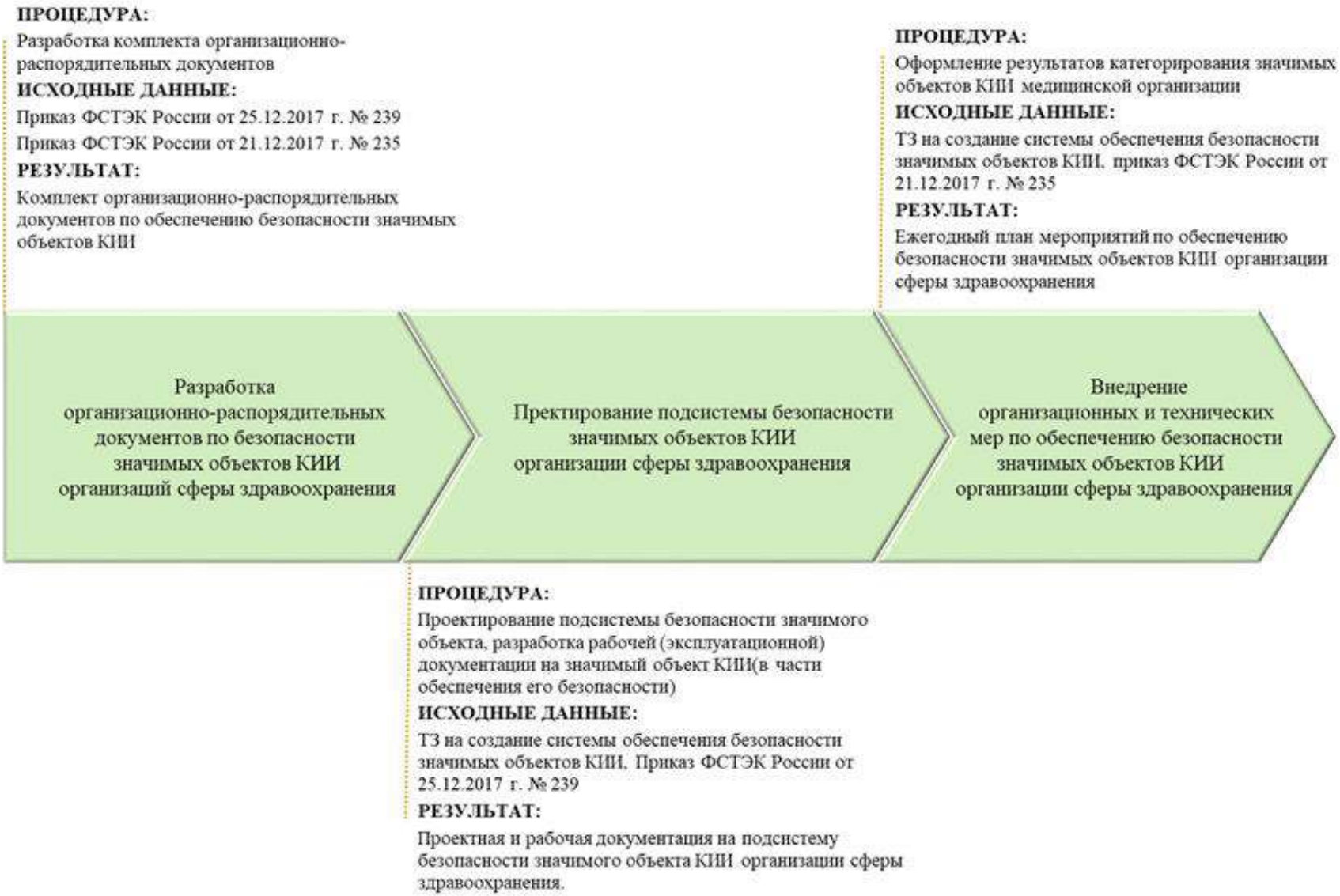
Состав и последовательность работ по обеспечению безопасности значимых объектов КИИ после завершения категорирования

Состав этапов создания подсистемы безопасности значимых объектов КИИ и организации взаимодействия

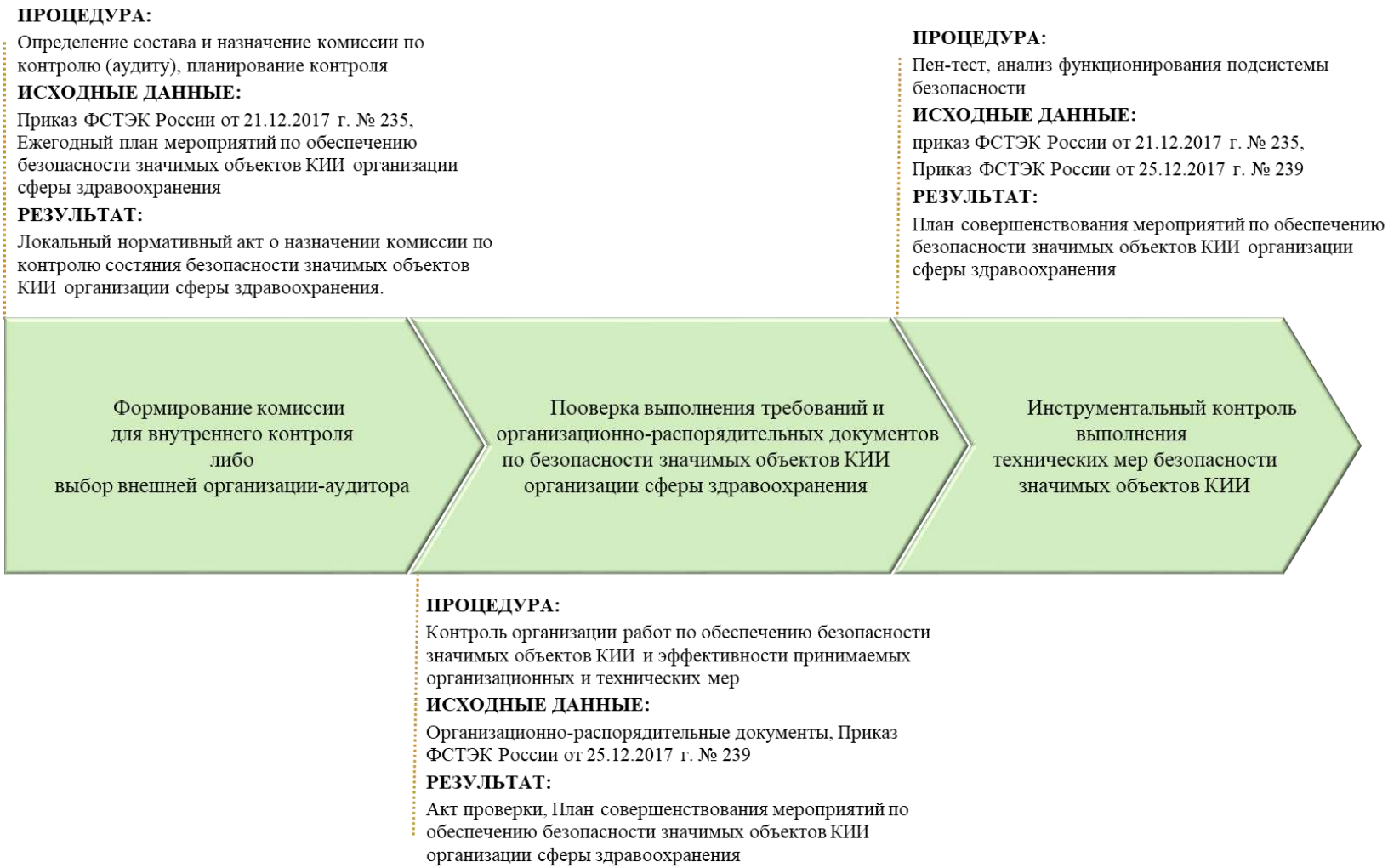


Состав процедур этапа «Планирование» создания подсистемы безопасности

Состав процедур этапа «Реализация» создания подсистемы безопасности



Состав процедур этапа «Контроль» создания подсистемы безопасности



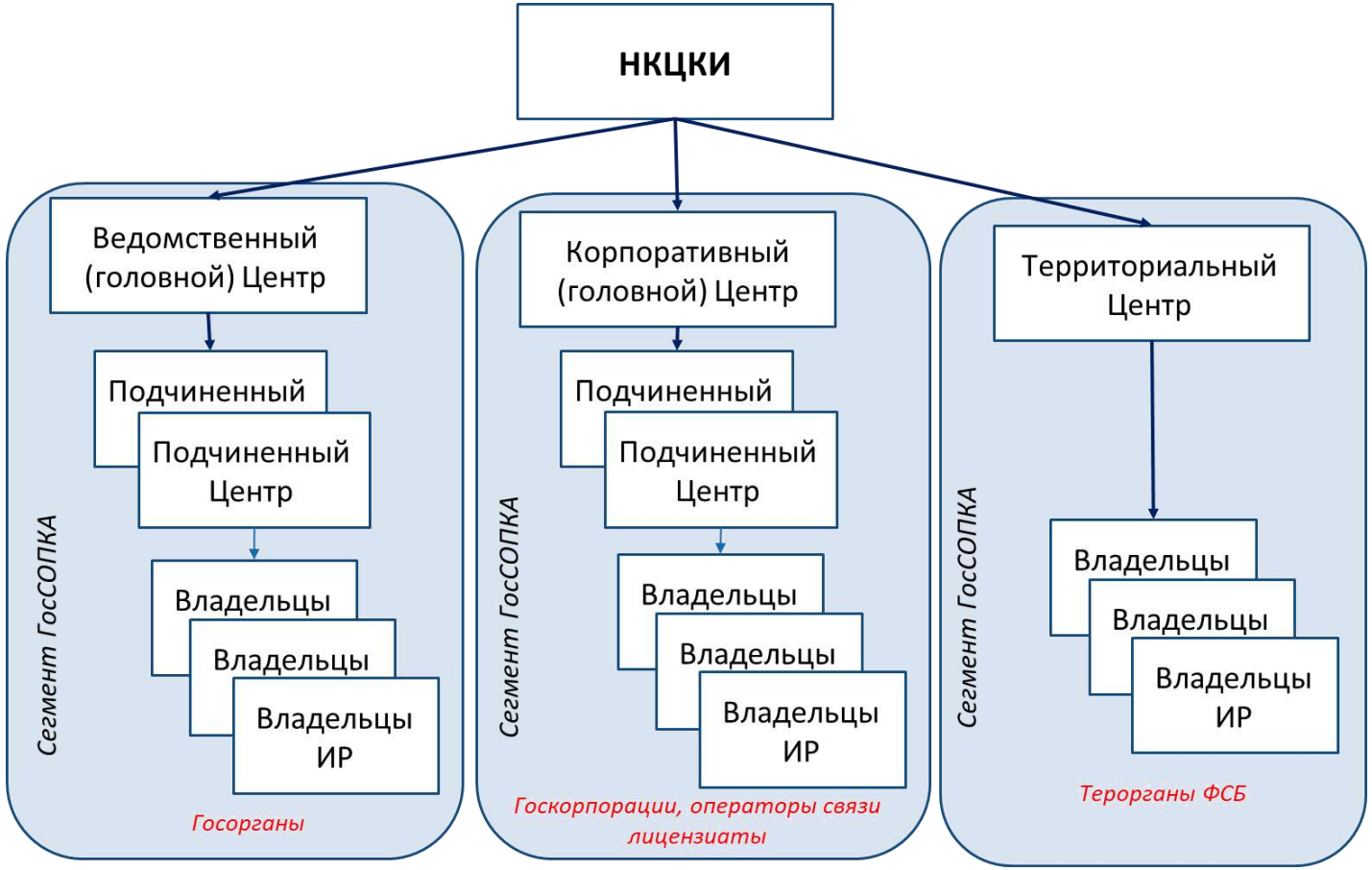
Приложение 19.

Перечень рекомендуемых организационно-распорядительных документов по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения

ОСНОВАНИЕ	ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЙ ДОКУМЕНТ
ФЗ-187, п.4, ч.1, ст. 9	План проведения мероприятий по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения
ФЗ-187, п.1, ч.2, ст. 9	План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак организации сферы здравоохранения
ФЗ-187, п.3, ч 3, ст. 9	Регламент реагирования на инциденты информационной безопасности в организации сферы здравоохранения
Пр. ФСТЭК № 235, п.8	Приказ назначении ответственных (подразделений) отвечающих за обеспечение безопасности КИИ
Пр. ФСТЭК № 235, п.9	Должностные обязанности должностных лиц (подразделений) при обеспечении безопасности значимых объектов КИИ
Пр. ФСТЭК № 235, п.22	Инструкция оператору, пользователю, системному администратору по применению средств защиты информации
Пр. ФСТЭК № 235, п.23	Положение, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ
Пр. ФСТЭК № 239, п.12.3	Правила (Регламент) разграничения доступа, определяющие права доступа субъектов доступа к объектам доступа
Пр. ФСТЭК № 239, п.13.5	Инструкция по реагированию на компьютерные инциденты
Пр. ФСТЭК № 239, п.13.6	План мероприятий по обеспечению безопасности значимого объекта КИИ на случай возникновения нештатных ситуаций

Приложение 20.

Общая структура Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)



Приложение 21.

Состав информации, передаваемой в рамках взаимодействия с Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)

ОСНОВАНИЕ	ОПИСАНИЕ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ	СРОК
п. 1 Порядка представления информации, утв. Приказом ФСБ России № 367	Информация, указанная в п. 1-4 Перечня информации, утв. Приказом ФСБ России № 367	Не реже 1 раза в месяц и не позднее месячного срока (при выполнении условий)
п. 4 Порядка информирования ФСБ России, утв. Приказом ФСБ России № 282 п. 5-6 Порядка представления информации, утв. Приказом ФСБ России № 367	Информация о компьютерных инцидентах	3 часа для значимого объекта КИИ 24 часа для иных объектов КИИ
п. 14 Порядка информирования ФСБ, утв. Приказом ФСБ России № 282	Информация о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак	48 часов
п. 7-9 Порядка представления информации, утв. Приказом ФСБ России № 367	Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты	Достаточный для своевременного реагирования на компьютерные инциденты