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 информационной 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)](https://internet.garant.ru/#/document/400699833/entry/1001), договора на право хозяйственного ведения[\*(2)](https://internet.garant.ru/#/document/400699833/entry/1002), договора на право оперативного управления[\*(3)](https://internet.garant.ru/#/document/400699833/entry/1003).

В соответствии с требованиями законодательства Российской Федерации, организации сферы здравоохранения как субъекты критической информационной 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 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](https://internet.garant.ru/#/document/71876120/entry/0) Правительства Российской Федерации от 08.02.2018 N 127, применительно к организациям сферы здравоохранения.

Перечень основных нормативных правовых актов, использованных при разработке настоящих методических рекомендаций, приведен в [Приложении 2](https://internet.garant.ru/#/document/400699833/entry/2000).

Перечень организаций сферы здравоохранения, на которые распространяется область действия настоящих методических рекомендаций, приведен в [Приложении 3](https://internet.garant.ru/#/document/400699833/entry/3000).

Примеры информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере здравоохранения, приведены в [Приложении 4](https://internet.garant.ru/#/document/400699833/entry/4000).

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

- определения состава бизнес-процессов[\*(4)](https://internet.garant.ru/#/document/400699833/entry/1004) в рамках видов деятельности организации сферы здравоохранения и выявления критических управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов организации сферы здравоохранения, нарушение или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим 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 критических процессов, или осуществляют управление, контроль или мониторинг критических 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](https://internet.garant.ru/#/document/400699833/entry/1000).

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](https://internet.garant.ru/#/document/71876120/entry/2011), [15-18](https://internet.garant.ru/#/document/71876120/entry/2015) Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных [постановлением](https://internet.garant.ru/#/document/71876120/entry/0) Правительства Российской Федерации от 08.02.2018 N 127.

Рекомендации по формированию постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры организации сферы здравоохранения приведены в [Приложении 5](https://internet.garant.ru/#/document/400699833/entry/5000).

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](https://internet.garant.ru/#/document/71730198/entry/7)[\*(5)](https://internet.garant.ru/#/document/400699833/entry/1005), а также [Правилами](https://internet.garant.ru/#/document/71876120/entry/1000) категорирования объектов критической информационной инфраструктуры Российской Федерации[\*(6)](https://internet.garant.ru/#/document/400699833/entry/1006) и [Перечнем](https://internet.garant.ru/#/document/71876120/entry/2000) показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными [постановлением](https://internet.garant.ru/#/document/71876120/entry/0) Правительства Российской Федерации от 08.02.2018 N 127.

9. Категорированию подлежат ИС, ИТКС, АСУ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные критические 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 критического 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.

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 критических;

- определение и формирование Перечня объектов КИИ, подлежащих категорированию, и выделение критических 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](https://internet.garant.ru/#/document/400699833/entry/6000).

2.2. Определение бизнес-процессов

13. Определение бизнес-процессов в деятельности организации сферы здравоохранения и выделение среди них критических 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](https://internet.garant.ru/#/document/400699833/entry/9000) критических бизнес-процессов в деятельности организации сферы здравоохранения.

Этапы определения бизнес-процессов организации сферы здравоохранения и их содержание приведены в [Приложении 6](https://internet.garant.ru/#/document/400699833/entry/6000).

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](https://internet.garant.ru/#/document/71876120/entry/0) Правительства РФ от 08.02.2018 N 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](https://internet.garant.ru/#/document/400699833/entry/7000).

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)](https://internet.garant.ru/#/document/400699833/entry/1007), транспортной инфраструктуры[\*(8)](https://internet.garant.ru/#/document/400699833/entry/1008), сетей связи[\*(9)](https://internet.garant.ru/#/document/400699833/entry/1009), а также, в дальнейшем, расчет 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)](https://internet.garant.ru/#/document/400699833/entry/1010) 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[\*(10)](https://internet.garant.ru/#/document/400699833/entry/1010) 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[\*(11)](https://internet.garant.ru/#/document/400699833/entry/1011), стратегическими предприятиями[\*(12)](https://internet.garant.ru/#/document/400699833/entry/1012), у которых возможно 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 возникновения ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации[\*(13)](https://internet.garant.ru/#/document/400699833/entry/1013), 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[\*(14)](https://internet.garant.ru/#/document/400699833/entry/1014) и (или) оказывает медицинские услуги, освобождаемые от налогообложения[\*(15)](https://internet.garant.ru/#/document/400699833/entry/1015).

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[\*(16)](https://internet.garant.ru/#/document/400699833/entry/1016), 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[\*(17)](https://internet.garant.ru/#/document/400699833/entry/1017).

26. Оценка критичности бизнес-процессов организации сферы здравоохранения, за исключением организаций сферы здравоохранения, использующих в своей деятельности источники ионизирующего излучения, с точки зрения экологической значимости[\*(18)](https://internet.garant.ru/#/document/400699833/entry/1018), 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[\*(19)](https://internet.garant.ru/#/document/400699833/entry/1019), 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[\*(20)](https://internet.garant.ru/#/document/400699833/entry/1020).

27. Оценка критичности бизнес-процессов организации сферы здравоохранения с точки зрения значимости для обеспечения обороны страны, безопасности государства и правопорядка[\*(21)](https://internet.garant.ru/#/document/400699833/entry/1021), 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](https://internet.garant.ru/#/document/400699833/entry/241) настоящих методических рекомендаций, могут быть использованы для 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[\*(22)](https://internet.garant.ru/#/document/400699833/entry/1022). 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 критическим, если в ходе оценки возможных последствий от его нарушения установлено, что он задействован и оказывает влияние хотя бы по одному критерию, определенному [постановлением](https://internet.garant.ru/#/document/71876120/entry/0) Правительства РФ от 08.02.2018 N 127.

Критерии влияния (задействованности) бизнес-процессов организации сферы здравоохранения на показатели возможных последствий приведены в [разделе I](https://internet.garant.ru/#/document/400699833/entry/8100) 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](https://internet.garant.ru/#/document/71876120/entry/0) Правительства РФ от 08.02.2018 N 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](https://internet.garant.ru/#/document/400699833/entry/8200) Справочных материалов по оценке критичности бизнес-процессов организации сферы здравоохранения (Приложение 8), для следующих показателей, определенных [постановлением](https://internet.garant.ru/#/document/71876120/entry/0) Правительства РФ от 08.02.2018 N 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[\*(23)](https://internet.garant.ru/#/document/400699833/entry/1023));

- 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;

- 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](https://internet.garant.ru/#/document/71876120/entry/0) Правительства РФ от 08.02.2018 N 127, используется [раздел](https://internet.garant.ru/#/document/400699833/entry/241) "Допущения и ограничения" настоящих методических рекомендаций.

36. В случае если осуществление критического бизнес-процесса организации сферы здравоохранения зависит от осуществления иных критических бизнес-процессов, оценка проводится исходя из совокупного масштаба возможных последствий от нарушения или прекращения функционирования всех выполняемых критических 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](https://internet.garant.ru/#/document/400699833/entry/7000)).

2.4.4. Формирование Перечня критических бизнес-процессов

38. После оценки критичности бизнес-процессов в деятельности организации сферы здравоохранения, из Реестра исключаются бизнес-процессы, которые не являются критическими, и формируется описательная часть Перечня критических бизнес-процессов организации сферы здравоохранения. Форма Перечня критических бизнес-процессов организации сферы здравоохранения представлена в [Приложении 9](https://internet.garant.ru/#/document/400699833/entry/9000).

2.5. Описание процесса "Определение и формирование Перечня объектов КИИ"

39. Процесс формирования Перечня объектов КИИ организации сферы здравоохранения и выделения критических 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 критических 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 критических приведен в [Приложении 6](https://internet.garant.ru/#/document/400699833/entry/6000).

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[\*(24)](https://internet.garant.ru/#/document/400699833/entry/1024) 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;

- 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](https://internet.garant.ru/#/document/400699833/entry/10000)).

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 критических бизнес-процессов организации сферы здравоохранения, и (или) осуществляют управление, контроль или мониторинг критических 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 критических бизнес-процессов организации сферы здравоохранения, и (или) осуществлении управления, контроля или мониторинга критических бизнес-процессов организации сферы здравоохранения;

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

44. Информационная система (ИС) считается задействованной в реализации критического бизнес-процесса организации сферы здравоохранения, если она предназначена для хранения, поиска и обработки информации, необходимой для выполнения основных функций критического бизнес-процесса, либо осуществляет управление, контроль или мониторинг критических 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;

|  |  |  |  |
| --- | --- | --- | --- |
| 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](https://internet.garant.ru/#/document/400699833/entry/17500) 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](https://internet.garant.ru/#/document/400699833/entry/17362) 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](https://internet.garant.ru/#/document/400699833/entry/17600) 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 |
|  | 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 |
|  | 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 |
|  | 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 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](https://internet.garant.ru/#/document/400699833/entry/17361) 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. Внутренний или внешний антропогенный (обслуживающий персонал, поставщик) 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 (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](https://internet.garant.ru/#/document/71730198/entry/1360), ч. 1, ст. 9 | План проведения мероприятий по обеспечению безопасности значимых объектов КИИ организации сферы здравоохранения |
| ФЗ-187, [п. 1](https://internet.garant.ru/#/document/71730198/entry/1361), ч. 2, ст. 9 | План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак организации сферы здравоохранения |
| ФЗ-187, [п. 3](https://internet.garant.ru/#/document/71730198/entry/1366), ч. 3, ст. 9 | Регламент реагирования на инциденты информационной безопасности в организации сферы здравоохранения |
| Пр. ФСТЭК N 235, [п. 8](https://internet.garant.ru/#/document/71886248/entry/1008) | Приказ назначении ответственных (подразделений) отвечающих за обеспечение безопасности КИИ |
| Пр. ФСТЭК N 235, [п. 9](https://internet.garant.ru/#/document/71886248/entry/1009) | Должностные обязанности должностных лиц (подразделений) при обеспечении безопасности значимых объектов КИИ |
| Пр. ФСТЭК N 235, [п. 22](https://internet.garant.ru/#/document/71886248/entry/1022) | Инструкция оператору, пользователю, системному администратору по применению средств защиты информации |
| Пр. ФСТЭК N 235, [п. 23](https://internet.garant.ru/#/document/71886248/entry/1023) | Положение, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ |
| Пр. ФСТЭК N 239, [п. 12.3](https://internet.garant.ru/#/document/71901880/entry/18) | Правила (Регламент) разграничения доступа, определяющие права доступа субъектов доступа к объектам доступа |
| Пр. ФСТЭК N 239, [п. 13.5](https://internet.garant.ru/#/document/71901880/entry/28) | Инструкция по реагированию на компьютерные инциденты |
| Пр. ФСТЭК N 239, [п. 13.6](https://internet.garant.ru/#/document/71901880/entry/29) | 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 системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)

|  |  |  |
| --- | --- | --- |
| Основание | Описание передаваемой информации | Срок |
| [п. 1](https://internet.garant.ru/#/document/72041504/entry/8) Порядка представления информации, утв. [Приказом](https://internet.garant.ru/#/document/72041504/entry/0) ФСБ России N 367 | Информация, указанная в [п. 1-4](https://internet.garant.ru/#/document/72041504/entry/1) Перечня информации, утв. [Приказом](https://internet.garant.ru/#/document/72041504/entry/0) ФСБ России N 367 | Не реже 1 раза в месяц и не позднее месячного срока (при выполнении условий) |
| [п. 4](https://internet.garant.ru/#/document/72298410/entry/1004) Порядка информирования ФСБ России, утв. [Приказом](https://internet.garant.ru/#/document/72298410/entry/0) ФСБ России N 282 [п. 5-6](https://internet.garant.ru/#/document/72041504/entry/12) Порядка представления информации, утв. [Приказом](https://internet.garant.ru/#/document/72041504/entry/0) ФСБ России N 367 | Информация о компьютерных инцидентах | 3 часа для значимого объекта КИИ 24 часа для иных объектов КИИ |
| [п. 14](https://internet.garant.ru/#/document/72298410/entry/1014) Порядка информирования ФСБ, утв. [Приказом](https://internet.garant.ru/#/document/72298410/entry/0) ФСБ России N 282 | Информация о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак | 48 часов |
| [п. 7-9](https://internet.garant.ru/#/document/72041504/entry/14) Порядка представления информации, утв. [Приказом](https://internet.garant.ru/#/document/72041504/entry/0) ФСБ России N 367 | Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты | Достаточный для своевременного реагирования на компьютерные инциденты |

|  |  |
| --- | --- |
| Заместитель Министра здравоохранения Российской Федерации | П.С. Пугачев |

Согласовано

|  |  |
| --- | --- |
| Директор Департамента цифрового развития и информационных технологий Министерства здравоохранения Российской Федерации | В.В. Ваньков |

5 апреля 2021 г.

Оглавление

|  |  |  |
| --- | --- | --- |
|  |  |  |

Свернуть

Name

|  |
| --- |
| Обозначения и сокращения |
| Введение |
| Определения |
| 1 Общие положения |
| 2 Методология формирования модели угроз |
| 3 Описание ИСПДн |
| 3.1 Определение условий создания и использования персональных данных |
| 3.2 Описание форм представления персональных данных |
| 3.3 Описание структуры ИСПДн |
| 3.4 Определение характеристик безопасности |
| 4 Пользователи ИСПДн |
| 5 Типы ИСПДн |
| 5.1 Характеристики ИСПДн |
| 5.2 Типизация ИСПДн |
| 6 Уровень исходной защищенности |
| 7 Вероятность реализации угроз безопасности |
| 7.1 Классификация угроз безопасности |
| 7.2 Классификация нарушителей |
| 7.3 Классификация уязвимостей ИСПДн |
| 7.4 Перечень возможных УБПДн |
| 7.5 Определение вероятности реализации УБПДн |
| 8 Реализуемость угроз |
| 9 Оценка опасности угроз |
| 10 Определение актуальности угроз в ИСПДн |
| Приложение 1. Обобщенная модель угроз для Автономной ИС I типа |
| Приложение 2. Обобщенная модель угроз для Автономной ИС II типа |
| Приложение 3. Обобщенная модель угроз для Автономной ИС III типа |
| Приложение 4. Обобщенная модель угроз для Автономной ИС IV типа |
| Приложение 5. Обобщенная модель угроз для Автономной ИС V типа |
| Приложение 6. Обобщенная модель угроз для Автономной ИС VI типа |
| Приложение 7. Обобщенная модель угроз для ЛИС I типа |
| Приложение 8. Обобщенная модель угроз для ЛИС II типа |
| Приложение 9. Обобщенная модель угроз для Распределенной ИС I типа |
| Приложение 10. Обобщенная модель угроз для Распределенной ИС II типа |

ДокументО документе

Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.)

Период действия 23.12.2009 - ?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Инструкция ответственного |
|  |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | | | | | |
| 2.3.1. Утрата ключей и атрибутов доступа | Низкая | Средняя | Средняя | Актуальная |  | Инструкция пользователя |
| Инструкция администратора безопасности |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | Маловероятно | Низкая | Низкая | Неактуальная | Настройка средств защиты | Резервное копирование |
| 2.3.3. Непреднамеренное отключение средств защиты | Маловероятно | Низкая | Низкая | Неактуальная | Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности | Инструкция пользователя |
| Инструкция администратора безопасности |
| 2.3.4. Выход из строя аппаратно-программных средств | Маловероятно | Низкая | Низкая | Неактуальная |  | Резервирование |
| 2.3.5. Сбой системы электроснабжения | Маловероятно | Низкая | Низкая | Неактуальная | Использование источника бесперебойного электропитания | Резервное копирование |
| 2.3.6. Стихийное бедствие | Маловероятно | Низкая | Низкая | Неактуальная | Пожарная сигнализация |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | | | | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке | Маловероятно | Низкая | Низкая | Неактуальная | Система защиты от НСД | Акт установки средств защиты |
| Разрешительная система допуска |
| Технологический процесс обработки |
|  |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Низкая | Средняя | Низкая | Неактуальная |  | Договор о не разглашении |
| Инструкция пользователя |
| 2.5. Угрозы несанкционированного доступа по каналам связи | | | | | | |
| 2.5.1. Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | | | | |  |  |
| 2.5.1.1. Перехват за переделами с контролируемой зоны; | Низкая | Средняя | Средняя | Актуальная | Шифрование | Технологический процесс |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями; | Маловероятно | Низкая | Низкая | Неактуальная | Шифрование | Пропускной режим |
| Физическая защита канала связи | Технологический процесс |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | Маловероятно | Низкая | Низкая | Неактуальная | Шифрование | Технологический процесс |
| Физическая защита канала связи |
| 2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | Низкая | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.3. Угрозы выявления паролей по сети. | Средняя | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.4. Угрозы навязывание ложного маршрута сети. | Низкая | Средняя | Низкая | Неактуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.5. Угрозы подмены доверенного объекта в сети. | Низкая | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях. | Низкая | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.7. Угрозы типа "Отказ в обслуживании". | Низкая | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Антивирусное ПО | Инструкция пользователя |
| Инструкция администратора безопасности |
| Резервирование |
| 2.5.8. Угрозы удаленного запуска приложений. | Средняя | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Антивирусное ПО | Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |
| 2.5.9. Угрозы внедрения по сети вредоносных программ. | Средняя | Средняя | Высокая | Актуальная | Антивирусное ПО | Технологический процесс |
| Инструкция пользователя |
| Инструкция администратора безопасности |
| Акт установки средств защиты |

Таким образом, актуальными угрозами безопасности ПДн в Распределенная ИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы наличия недекларированных возможностей системного ПО и ПО для обработки персональных данных;

- угрозы перехвата за переделами с контролируемой зоны

- угрозы сканирования;

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы подмены доверенного объекта в сети;

- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

- угрозы типа "Отказ в обслуживании";

- угрозы удаленного запуска приложений;

- угрозы внедрения по сети вредоносных программ;

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;

- сертификация программных средств на НДВ;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн;

- осуществление резервирования ключевых элементов ИСПДн;

- организация физической защиты каналов передачи данных;

- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;

- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.