«УТВЕРЖДАЮ»
Главный врач
государственного учреждения
здравоохранения Ярославской
области «ГОРОДСКАЯ
ДЕТСКАЯ БОЛЬНИЦА»
_____В.А. Логинов
«18» ноября 2019 г.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных государственного учреждения здравоохранения Ярославской области «ГОРОДСКАЯ ДЕТСКАЯ БОЛЬНИЦА»

1. Общие положения

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» иустанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) исходя из Требований к защите персональных данных при их обработке в информационных системах персональных данных государственного учреждения здравоохранения Ярославской области «ГОРОДСКАЯ ДЕТСКАЯ БОЛЬНИЦА» как Оператора по обработке персональных данных (далее Оператор), утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

   Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система, ИСПДн) обеспечивает Оператор или лицо, осуществляющее обработку персональных данных по поручению Оператора в соответствии с законодательством Российской Федерации.

   Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Россий-

ской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, созданной в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, и направлены на нейтрализацию актуальных угроз безопасности персональных данных.
4. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

11. Состав и содержание мер по обеспечению безопасности персональных данных

5. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

Организационные меры Оператора обеспечения безопасности персональных данных:

-назначение приказом ответственных лиц за организацию обработки персональных данных, руководство выполнением работ по комплексной защите информации, обеспечение эффективного применения имеющихся организационных и инженерно-технических мер по защите информации, обеспечение контроля за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации и координации деятельности подразделений по защите информации;

-установка перечня должностных групп (лиц), осуществляющих обработку персональных данных либо имеющих к ним доступ;

-обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

-ограничение доступа лиц в помещения, в которых ведется работа с персональными данными, обеспечение сохранности носителей персональных данных и средств защиты информации, исключение возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

-ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников;

-учет машинных носителей персональных данных.

6. В состав технических мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных входят:

идентификация и аутентификация сотрудников и объектов доступа;
управление доступом сотрудников к объектам доступа;
защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
регистрация событий безопасности;
антивирусная защита;
предотвращение вторжений;
контроль и анализ защищенности персональных данных;
обеспечение целостности информационной системы и персональных данных;
обеспечение доступности персональных данных;
защита технических средств;
защита информационной системы, ее средств, систем связи и передачи данных;
выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
управление конфигурацией информационной системы и системы защиты персональных данных.

8. Состав и содержание мер Оператора по обеспечению безопасности персональных данных, приведены в таблице:

№ п/п	Меры по защите информации.
1	Идентификация и аутентификация пользователей.
2	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
3	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей). Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних ползователей
4	Реализация правил разграничения доступа.
5	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системой.
6	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
7	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему.
9	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
10	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.
11	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
12	Регламентация и контроль использования в информационной системе технологий беспроводного доступа.
13	Регламентация и контроль использования в информационной системе мобильных технических средств.

14	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
15	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.
16	Определение событий безопасности, подлежащих регистоации, и сроков их хранения.
17	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
18	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.
19	Защита информации о событиях безопасности.
20	Реализация антивирусной защиты.
21	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
22	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.
23	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.
24	Контроль работоспособности параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.
25	Контроль состава технических средств, программного обеспечения и средств защиты информации.
26	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
27	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.
28	Регистрация событий безопасности в виртуальной инфраструктуре.
29	Реализация и управление антивирусной защитой в виртуальной инфраструктуре.
30	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.
31	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.
32	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.
33	Защита беспроводных соединений, применяемых в информационной системе.
34	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.
35	Управление изменениями конфигурации информационной системы и системы защиты персональных данных.
36	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных.

37	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

9. Меры по идентификации и аутентификации сотрудников и объектов доступа обеспечивают присвоение сотрудникам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого сотрудником идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности сотруднику предъявленного им идентификатора (подтверждение подлинности).
10. Меры по управлению доступом сотрудников к объектам доступа обеспечивают управление правами и привилегиями сотрудников, разграничение доступа сотрудников к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивают контроль за соблюдением этих правил.
11. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключают возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.
12. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.
13. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
14. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
15. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.
16. Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.
17. Меры по обеспечению целостности информационной системы и персональных данных обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

18. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ сотрудников, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.
19. Меры по защите среды виртуализации исключают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.
20. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий.
21. Меры по защите информационной системы, ее средств, систем связи и передачи данных обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.
22. Меры по выявлению инцидентов и реагированию на них обеспечивают обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.
23. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.