УТВЕРЖДАЮ

Главный врач

ГБУЗ «Госпиталь для ветеранов войн»

_____ О.С. Сухарев

«__01__» _____ 202_г.

ПОЛОЖЕНИЕ
по организации и проведению работ
по обеспечению безопасности конфиденциальной информации
при их обработке в информационных системах
ГБУЗ «Госпиталь для ветеранов войн»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности конфиденциальной информации при их обработке в информационных системах ГБУЗ «Госпиталь для ветеранов войн» (далее – Положение) разработано в соответствии с Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности информации, содержащей сведения конфиденциального характера ГБУЗ «Госпиталь для ветеранов войн» (далее – Учреждение).

1.3. Настоящее Положение устанавливает порядок обращения в Учреждении с информацией, содержащей сведения конфиденциального характера с использованием средств автоматизации или без использования таких средств, а также регулирует права и обязанности работников и работодателя в области защиты информации.

1.4. Отнесение сведений к категории конфиденциальной информации осуществляется в соответствии с Перечнем сведений конфиденциального характера в ГБУЗ «Госпиталь для ветеранов войн» (далее – Перечень).

1.5. Действие настоящего Положения не распространяется на правоотношения, связанные с обращением со сведениями, составляющими государственную тайну.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

Доступность информации – состояние информации и ее носителей, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.

Информация, содержащая сведения конфиденциального характера (конфиденциальная информация, конфиденциальные данные) – врачебная, коммерческая, банковская, налоговая тайны, а также персональные данные, обрабатываемые в Учреждении. Определяется Перечнем сведений конфиденциального характера и Перечнем персональных данных, обрабатываемых в Учреждении.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность информации – обязательное для соблюдения Учреждением или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы (далее – ИС).

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы, или использующее результаты ее функционирования.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

3. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ КОНФИДЕНЦИЛЬНОГО ХАРАКТЕРА

3.1. К работе со сведениями, содержащими конфиденциальную информацию, допускаются работники Учреждения, заключившие трудовой договор, содержащий соответствующее условие о неразглашении конфиденциальной информации.

3.2. Внутри Учреждения особый порядок обращения с этой категорией информации, как правило, не предусматривается, т.е. он может оставаться таким же, как и для открытой информации.

3.3. При возникновении необходимости направления конфиденциальной информации за пределы Учреждения, либо в случае установления исполнителем документа особого порядка его обращения внутри Общества, на документе (его электронном аналоге) проставляется гриф конфиденциальности.

Дальнейшая работа с такого рода документами осуществляется в соответствии с требованиями Порядка обращения со служебной информацией ограниченного распространения в Министерстве здравоохранения Республики Карелия и подведомственных учреждениях.

3.4. Порядок обработки персональных данных (обращения с информацией, содержащей персональные данные) определяется законодательством Российской Федерации, нормативными правовыми актами в области защиты информации, Политикой в отношении обработки персональных данных в ГБУЗ «Госпиталь для ветеранов войн» и внутренними документами Учреждения.

4. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Под организацией обеспечения безопасности конфиденциальной информации понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности, реализуемых в рамках создаваемой системы защиты информации.

4.2. Система защиты информации включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

4.3. Система защиты информации должна обеспечить целостность, конфиденциальность и доступность информации.

4.4. Безопасность ПДн при их обработке в ИСПДн обеспечивает Учреждение или лицо, осуществляющее обработку ПДн по поручению Учреждения на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Учреждением и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4.5. Выбор мер и средств защиты информации для системы защиты осуществляется Учреждением в соответствии с нормативными правовыми актами, принятыми, в том числе, Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России).

4.6. Структура, состав и основные функции системы защиты информации определяются, в том числе, исходя из уровня защищенности ПДн при их обработке в ИСПДн.

4.7. Модернизация системы защиты информации для функционирующих информационных систем, в том числе ИСПДн, Учреждения должна осуществляться в случае:

- изменения состава или структуры ИС или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки данных, топологии ИС):
- изменения состава угроз безопасности данным в ИС;
- изменения уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению Учреждения.

4.8. В целях определения необходимости доработки (модернизации) системы защиты информации не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться инвентаризация информационных систем Учреждения, проверка состава и структуры ИСПДн, состава угроз безопасности и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Учреждения.

4.9. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПДн;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) данных или другим нарушениям, приводящим к снижению уровня защищенности;
- нарушение заданного уровня безопасности данных (конфиденциальность/ целостность/доступность).

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5.1. Работы по обеспечению безопасности конфиденциальной информации проводятся в соответствии с Планом мероприятий по защите информации, утверждаемом главным врачом Учреждения. Внутренние проверки соответствия обработки и защиты информации Учреждением проводятся в соответствии с Правилами проведения внутреннего контроля соответствия обработки конфиденциальной информации. По результатам проведения внутренней проверки оформляется Протокол проведения внутреннего контроля соответствия обработки конфиденциальной информации требованиям защиты информации в ГБУЗ «Госпиталь для ветеранов войн».

5.2. Контроль за проведением работ по обеспечению безопасности персональных данных осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите персональных данных, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн Учреждения требованиям безопасности персональных данных.

5.3. При необходимости к проведению работ по обеспечению безопасности конфиденциальной информации, в том числе персональных данных, могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

5.4. В соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании систем защиты информации средств криптографической защиты информации к проведению работ по обеспечению безопасности информации Учреждению необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

6. ОТВЕТСТВЕННОСТЬ

6.1. Требования настоящего Положения обязательны для исполнения всеми работниками Учреждения, которые несут персональную ответственность за сохранность сведений конфиденциального характера, за соблюдение принятых организационных и технических мер защиты информации.

6.2. Руководители структурных подразделений Учреждения несут ответственность за организацию работы с документами, содержащими конфиденциальную информацию, а также за соблюдение принятых организационных и технических мер защиты информации в подчиненных им подразделениях.

6.3. Работники Учреждения, допустившие утечку сведений, содержащих конфиденциальную информацию, либо нарушившие требования настоящего Положения и других распорядительных документов, устанавливающих порядок обращения со сведениями, содержащими конфиденциальную информацию или порядок защиты таких сведений, а также работники, по вине которых произошла утрата носителей конфиденциальной информации, несут ответственность предусмотренную законодательством Российской Федерации, внутренними документами Учреждения и условиями трудового договора.

6.4. Ответственность лиц, не являющихся работниками Учреждения, за утечку или утрату сведений, содержащих конфиденциальную информацию, доверенных им в связи с участием в деятельности Учреждения, устанавливается соглашениями о взятии ими на себя таких обязательств и законодательством Российской Федерации.