МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ

государственное бюджетное учреждение здравоохранения Архангельской области
«КОРЯЖЕМСКАЯ ГОРОДСКАЯ БОЛЬНИЦА»

П Р И К А З

от 05 июля 2023 № 346 г.Коряжма Архангельской области

О положении о защите информации
ГБУЗ АО «Коряжемская городская больница»

Руководствуясь Федеральным законом «О персональных данных» от 27.07.2006 г. № 152-ФЗ

ПРИКАЗЫВАЮ:

1. Утвердить положение о защите информации ГБУЗ АО «Коряжемская городская больница» (прилагается).
2. Признать утратившим силу приказ О положении о защите информации ГБУЗ АО «Коряжемская городская больница» от 15.12.2017 №824.

И.О главного врача О.К Креминь

Приложение
Утверждено
приказом от « 05 » июля 2023г. № 346

Положение о защите информации
ГБУЗ АО «Коряжемская городская больница»

1. Общие положения

1.1 Настоящее Положение по защите информации (далее по тексту - Положение) устанавливает единый порядок и основные требования по обеспечению защиты информации, собираемой, обрабатываемой и хранимой с применением средств вычислительной техники (далее по тексту - СВТ) в государственном бюджетном учреждении здравоохранения Архангельской области «Коряжемская городская больница» (далее по тексту - учреждение) и является обязательным для выполнения всеми сотрудниками учреждения.

1.2. Положение разработано в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных».

1.3. В Положении используются следующие основные понятия:

информация – сведения (сообщения, данные) независимо от формы их предоставления;

информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

документированная информация (документ) – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа;

пользователь – сотрудник учреждения, пользующийся услугами информационной системы для получения информации или решения других задач.

1.4. Цели защиты информации в учреждении:

1. предотвращение или существенное затруднение несанкциониро-

ванного получения информации ограниченного доступа, ее уничтожения, искажения или модификации, создание у нарушителя ложного представления об истинной информации, а также предотвращение нарушения работы средств и систем информации и связи в учреждении;

2. защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационной системе учреждения;
3. сохранение конфиденциальности документированной информации в соответствии с законодательством.

1.5. Основными направлениями защиты информации являются:

1 обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней;

2 обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

1.6. Защите подлежат:

- информационные ресурсы, содержащие сведения, отнесенные к информации ограниченного доступа, представленные в виде носителей на магнитной и оптической основе, информативных физических полей, информационных массивов и баз данных.

К защищаемым информационным ресурсам относятся:

- база данных медицинской информационной системы «Ариадна»,
- база данных программного обеспечения «Льготное лекарственное обеспечение»,
- база данных программного комплекса «Высокотехнологичная медицинская помощь»,
- федеральный регистр медицинских и фармацевтических работников,
- база данных застрахованных лиц,
- регистры пациентов,
- регистр региональных льготников,
- регистр больных хроническими заболеваниями,
- база данных детей, прошедших диспансеризацию,
- другие сведения ограниченного доступа.

- средства и информационные технологии (СВТ, информационно-вычислительные комплексы, сети и системы), программное обеспечение (операционные системы, системы управления базами данных, другое общесистемное и прикладное ПО), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные, телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации ограничен-

ного доступа.

1.7. Основные угрозы безопасности информации:

- нарушение целостности обрабатываемой информации (искажение и уничтожение информации, ошибки в программном обеспечении). Целостность информации может быть нарушена как злоумышленником, так и неквалифицированными действиями пользователя или обслуживающего персонала, а также во время передачи информации по каналам связи;
- нарушение конфиденциальности обрабатываемой информации (несанкционированный доступ к информации);
- нарушение работоспособности автоматизированной информационной системы, локальной вычислительной сети (ЛВС) и ПЭВМ.

1.8. Защита информации в учреждении достигается комплексным применением организационно-технических мер и программно-аппаратных средств защиты и контроля:

а) выполнением требований нормативных документов по обеспечению защиты информации;

б) организацией резервного копирования, восстановления и архивирования данных;

в) установлением ответственности должностных лиц учреждения за обеспечение безопасности информации;

г) выделением штатного специалиста для непосредственного выполнения комплекса работ по защите информации;

д) контролем над применением средств копирования, хранения и стирания информации, функционированием средств защиты, соблюдением требований по обеспечению защиты информации сотрудниками учреждения.

2. Обязанности должностных лиц по обеспечению защиты информации

2.1. Общее руководство организацией защиты информации и контроль над ее состоянием осуществляет главный врач учреждения.

2.2. Ответственность за организацию и выполнение мероприятий по обеспечению защиты информации возлагается на главного врача учреждения.

Главный врач учреждения обязан:

- определять функциональные обязанности работников учреждения с учетом их персональной ответственности за состояние безопасности информации, обрабатываемой на СВТ;
- назначать специалиста, ответственного за защиту информации в учреждении, и контролировать его работу;
- обеспечить взаимодействие с государственным бюджетным учреждением здравоохранения Архангельской области «Медицинский информационно-аналитический центр» по вопросам обработки (сбор, накопление, хранение, использование, распространение, передача и уничтожение) персональных данных и другой информации ограниченного доступа.

2.3. Практическая реализация мероприятий и контроль соблюдения требований по защите информации в учреждении организуется и осуществляется

специалистом, ответственным за защиту информации в учреждении.

2.4. На специалиста, ответственного за защиту информации, возлагаются следующие обязанности:

- разработка проектов приказов, инструкций и рекомендаций по обеспечению защиты информации в учреждении и осуществление контроля их выполнения;

- установка и настройка программно-аппаратного обеспечения по обработке и защите информации, а именно:

  - средств криптографической защиты информации (ViPNet),
  - средств защиты от несанкционированного доступа к информации,
  - антивирусного программного обеспечения,
  - средств разграничения доступа и полномочий пользователей в операционных системах, базах данных, локальных вычислительных сетях и т.д.;

- выработка и выдача пользователям паролей на включение ПЭВМ, вход в ЛВС, доступ к базам данных в соответствии со специальными требованиями:

- осуществление антивирусной защиты информационной системы учреждения, контроль над защитой от несанкционированного доступа;

- контроль над соблюдением пользователями своих полномочий по доступу к СВТ, в ЛВС и базы данных;

- создание надлежащих условий для безопасности сохранения СВТ, машинных и бумажных носителей информации;

- выбор общесистемного программного обеспечения, оценка уровня защиты информации при его использовании. Установка и настройка на СВТ только лицензионного программного обеспечения. Формирование и предоставление главному врачу учреждения планов по обновлению действующих лицензий (по мере возникновения необходимости);

- разработка процедур сохранения-восстановления информации, выбор соответствующего программного обеспечения;

- обеспечение требований защиты информации при работе с базами данных, зарегистрированными в учреждении, их копировании и архивировании, при обмене данными;

- проведение совещаний по вопросам обеспечения защиты информации в учреждении и консультирование пользователей;

- организация расследований по фактам нарушения требований защиты информации в учреждении и предоставление результатов главному врачу учреждения для принятия соответствующих мер.

2.5. Персональную ответственность за выполнение установленных правил и требований по обеспечению безопасности информации, обрабатываемой в учреждения, несет пользователь.

Пользователь обязан:

- соблюдать требования распорядительных и нормативно-методических документов, регламентирующих порядок обеспечения защиты информации, в том числе настоящего Положения;

- строго хранить информацию ограниченного доступа;

- хранить на персональном компьютере (далее – ПК) сведения, отнесенные к информации ограниченного доступа, в минимально-необходимом для работы специалиста объеме;

- соблюдать правила по обеспечению защиты информации при использовании паролей при работе на ПК (доступ в операционную систему, в базу данных и т.д.):

- немедленно сообщать своему непосредственному начальнику и специалисту, ответственному за защиту информации, обо всех замеченных несанкционированных изменениях в аппаратной и программной конфигурации ПК.

Пользователю запрещается:

- проводить работы, связанные с решением задач конфиденциального характера, без выполнения установленных мероприятий по защите информации;

- разглашать сведения ограниченного доступа;

- работать с программами, обрабатывать информацию, производить печать и операции с файлами, если это не входит в круг должностных обязанностей пользователя;

- уничтожать, копировать или производить какие-либо другие действия со сведениями, отнесенными к информации ограниченного доступа, кроме действий выполняемых специалистом в рамках должностных обязанностей;

- самостоятельно производить настройки программного и аппаратного обеспечения по защите информации (политики безопасности и права учетной записи в операционной системе, антивирусное программное обеспечение и т.д.).

3. Допуск к информации ограниченного доступа

3.1. Все сотрудники, принятые на работу в учреждение, обязаны изучить нормативные документы по защите информации в части, их касающейся.

3.2. Работники, допущенные к информации ограниченного доступа, несут личную ответственность за соблюдение ими установленного в учреждении режима защиты информации и обязаны строго соблюдать сохранность сведений ограниченного доступа, не допускать действий, подрывающих или дискредитирующих авторитет организации.

3.3. Допуск сотрудников учреждения к информации ограниченного доступа осуществляется после изучения ими требований Положения и других нормативных документов по защите информации в части, их касающейся.

3.4. Работникам, допущенным к информации ограниченного доступа, запрещается сообщать устно или письменно кому бы то ни было сведения, содержащиеся на машинных носителях информации и документах, если это не вызывается служебной необходимостью.

3.5. За разглашение сведений, относящихся к информации ограниченного доступа, утрату машинных носителей информации, содержащих такие сведения, либо за иные нарушения режима защиты информации виновные лица привлекаются к ответственности в соответствии с действующим законодательством.