Приложение №3
к приказу от 23.07.2025
№ 254 краевого
государственного бюджетного
учреждения здравоохранения
«Краевая клиническая
больница» имени профессора
С.И. Сергеева
от №

Положение о защите информации, обрабатываемой в информационных системах краевого государственного бюджетного учреждения здравоохранения «Краевая клиническая больница» имени профессора С.И. Сергеева

1. Используемые понятия

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники от внутренних или внешних угроз, при котором обеспечены ее конфиденциальность, доступность и целостность.

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами, за исключением сведений, составляющих государственную тайну.

Конфиденциальность информации – состояние информации (ресурсов информационной системы), при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Оператор информационной системы – государственный орган, муниципальный орган, юридическое или физическое лицо, организующий и (или) осуществляющий деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Средства криптографической защиты информации – средства защиты информации, реализующее алгоритмы криптографического преобразования информации.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

Целостность информации – состояние защищенности информации, характеризуемое способностью обеспечивать сохранность и неизменность защищаемой информации при попытках несанкционированного или случайного воздействия на нее в процессе обработки или хранения.

2. Общие положения

Настоящее положение о защите информации, обрабатываемой в информационных системах краевого государственного бюджетного учреждения здравоохранения «Краевая клиническая больница» имени профессора С.И. Сергеева (далее – Положение), разработано на основании:

1) Федерального закона Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2) Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

3) Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4) Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17.

5) Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 №21.

Положение определяет порядок организации и проведения работ по защите информации, обрабатываемой в информационных системах краевого государственного бюджетного учреждения здравоохранения «Краевая клиническая больница» имени профессора С.И. Сергеева (далее – ИС).

Обладатель информации, оператор и владелец ИС определяются в техническом паспорте на каждую информационную систему.

Положение предназначено для работников краевого государственного бюджетного учреждения здравоохранения «Краевая клиническая больница» имени профессора С.И. Сергеева (далее – КГБУЗ ККБ имени С.И. Сергеева), операторов ИС и сторонних организаций, допускаемых в установленном порядке к выполнению работ на основных технических средствах и системах ИС, а также по модернизации их оборудования и программного обеспечения.

Ответственность за выполнение требований Положения возлагается на всех операторов ИС.

Положение вступает в силу с момента его утверждения главным врачом КГБУЗ ККБ имени С.И. Сергеева и действует бессрочно, до замены его новым положением.

3. Тип обрабатываемой информации в ИС

В ИС осуществляется обработка служебной информации (информация о функционировании оператора ИС и (или) КГБУЗ ККБ имени С.И. Сергеева, не отнесенная к категории общедоступной или конфиденциальной) и общедоступной информации (общеизвестные сведения и иная информация, доступ к которой не ограничен (ст. 7 Федерального закона Российской Федерации №149-ФЗ).

В ИС допускается обработка персональных данных (в соответствии с пунктами 1 (персональные данные) и 4 (врачебная тайна) сведений конфиденциального характера, утвержденных Указом Президента Российской Федерации от 06.03.1997 №188).

4. Цели создания системы защиты информации

Целью создания системы защиты информации (далее – СЗИ) в ИС является:

1) предотвращение ущерба (возникновение которого возможно в результате утери, хищения, утраты, искажения, подделки информации в любом ее проявлении);

2) реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации Российской Федерации.

Для информации, обрабатываемой в ИС, требуется обеспечить ее конфиденциальность, целостность и доступность.

5. Основные направления работ по обеспечению безопасности информации

Основными направлениями работ по обеспечению безопасности информации в ИС являются:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

2) разработка и практическая реализация организационных и технических мероприятий по защите информации;

3) своевременное обнаружение фактов несанкционированного доступа к информации;

4) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

5) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

6) обеспечение возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

7) осуществление постоянного контроля за обеспечением класса и уровня защищенности ИС.

6. Основные способы и меры по обеспечению безопасности информации

Основными способами и мерами по обеспечению безопасности информации в ИС являются:

1) привлечение лицензиатов ФСТЭК России для выполнения работ по технической защите информации;

2) противодействие утечке по техническим каналам, несанкционированному доступу, программно-техническому воздействию с целью нарушения конфиденциальности, целостности и доступности информации в процессе ее обработки, передачи и хранения;

3) применение автоматизированных систем в защищенном исполнении для обработки, хранения и передачи информации;

4) использование средств защиты информации, сертифицированных ФСТЭК России и ФСБ России, и контроль их эффективности;

5) аттестация ИС по требованиям безопасности информации.

7. Порядок обработки информации в ИС

Определение необходимых класса и (или) уровня защищенности ИС осуществляется комиссией, сформированной из числа работников оператора и (или) КГБУЗ ККБ имени С.И. Сергеева. В комиссию должны входить не менее трех человек.

По завершении процедуры классификации составляется Акт классификации ИС.

На этапе проведения процедур классификации ИС комиссией определяется состав информации, подлежащей защите, формируется перечень защищаемых информационных ресурсов в ИС.

Для ИС распоряжением (приказом) руководителя оператора и (или) главным врачом КГБУЗ ККБ имени С.И. Сергеева назначается лицо или подразделение, ответственное за организацию защиты информации в ИС (далее – администратор ИБ).

Администратор ИБ в своей деятельности руководствуется Инструкцией администратора информационной безопасности.

К техническому обслуживанию средств и систем ИС допускаются только лица, внесенные в списки лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Любые изменения в конфигурации ИС, влияющие на класс защищенности, должны быть учтены администратором ИБ в Журнале регистрации изменений в конфигурации информационной системы.

На основные технические средства и системы ИС может быть проведена инсталляция программного обеспечения исключительно указанного в перечне программного обеспечения, разрешенного к установке в ИС, который разрабатывает администратор ИБ.

Администратор ИБ составляет Технический паспорт ИС по форме, установленной в Порядке организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утвержден приказом
ФСТЭК России от 29.04.2021 №77). Затем паспорт ИС утверждается руководителем оператора и (или) главным врачом КГБУЗ ККБ имени С.И. Сергеева.

В ИС все машинные носители информации, в том числе съемные, подлежат учету.

В случае, если в ИС имеется разграничение прав доступа пользователей к информации, администратор ИБ разрабатывает Разрешительную систему доступа к информационным ресурсам ИС с указанием субъектов и объектов доступа.

Для определения вероятных нарушителей и актуальных угроз безопасности для ИС разрабатывается Модель угроз безопасности ИС. При необходимости к разработке Модели угроз безопасности ИС могут привлекаться организации-лицензиаты ФСТЭК и ФСБ России.

Ежегодно администратор ИБ разрабатывает и (или) актуализирует план мероприятий по обеспечению защиты информации в ИС на текущий год, который согласуется с руководителем оператора и (или) главным врачом КГБУЗ ККБ имени С.И. Сергеева.

Администратор ИБ производит учет всех мероприятий, направленных на обеспечение безопасности информации, обрабатываемой в ИС, в Журнале учета мероприятий по защите информации в ИС.

Не допускается обработка информации ИС при отсутствии в ней:

1) установленных и настроенных средств защиты информации, сертифицированных ФСТЭК России и (или) ФСБ России;

2) утвержденных организационных документов о порядке эксплуатации ИС.

При обработке информации в ИС запрещается:

1) вносить несогласованные изменения в ИС, которые могут снизить класс и (или) уровень защищенности информации;

2) проводить обработку информации без выполнения всех мероприятий по ее защите;

3) допускать к обработке информации лиц, не оформленных в установленном порядке;

4) производить копирование информации на неучтенные машинные носители информации, в том числе для временного хранения информации;

5) обрабатывать информацию на технических средствах в составе ИС при обнаружении каких-либо неисправностей, а также при отключенных средствах защиты информации;

6) обрабатывать защищаемую информацию на технических средствах при окончании сроков действия сертификатов средств защиты информации, за исключением окончания срока действия сертификатов соответствия при условии соблюдения требований по безопасности информации и при наличии действующей технической поддержки на средства защиты информации;

7) передавать защищаемую информацию за пределы контролируемой зоны по открытым каналам связи.

8. Ответственность за нарушение норм, регулирующих обработку и защиту информации в ИС

Лицо (подразделение), разрешающее доступ работников к защищаемой информации, несет персональную ответственность за это разрешение.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту информации в ИС, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами Российской Федерации, а также привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами Российской Федерации.

9. Заключительные положения

Администратор ИБ и пользователи, допущенные к работе в ИС, обязаны ознакомиться с Положением.

Администратор ИБ совместно с лицом (подразделением), ответственным за защиту информации в ИС, обязаны пересматривать и приводить в соответствие положения настоящего документа в случае изменения законодательства Российской Федерации в области защиты информации.

10. Нормативно-правовые акты и методические документы по защите информации

1) Конституция Российской Федерации.

2) Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3) Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

4) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06.03.1997 №188.

5) Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 01.11.2012 №1119).

6) Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 №17.

7) Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18.02.2013 №21).

8) Методический документ «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России от 11.02.2014).

9) Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена приказом ФАПСИ России от 13.06.2001 №152).

10) Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств (утверждены приказом ФСБ России от 24.10.2022 №524).

11) Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России от 31.03.2015 №149/7/2/6-432).