Министерство здравоохранения Пермского края
Государственное бюджетное учреждение
здравоохранения Пермского края
«Ордена «Знак Почета» Пермская краевая клиническая больница»
(ГБУЗ ПК «Пермская краевая клиническая больница»)

ПРИКАЗ

«25» апреля 2019г. № 72

г. Пермь

Об утверждении «Политики информационной безопасности» и «Модели угроз и нарушения безопасности персональных данных»

На основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказов ФСТЭК от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», 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»

ПРИКАЗЫВАЮ:

1. Утвердить «Политику информационной безопасности в ГБУЗ ПК «Пермская краевая клиническая больница» (приложение № 1).
2. Утвердить «Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных ГБУЗ ПК «Пермская краевая клиническая больница»
3. Начальнику информационно-вычислительного центра Мохиреву Д.А. осуществлять общий контроль состояния информационной безопасности ГБУЗ ПК «Пермская краевая клиническая больница»
4. Секретарю главного врача ознакомить с настоящим приказом руководителей структурных подразделений.
5. Специалисту отдела кадров Флягиной З.А. опубликовать Политику информационной безопасности ГБУЗ ПК «Пермская краевая клиническая больница» на официальном сайте больницы в сети Интернет.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А.В. Касатов

УТВЕРЖДЕНО
Главный врач
ГБУЗ ПК
«Пермская краевая клиническая больница»
Касатов А. В.
от «25» 04 2019 г.

Политика информационной безопасности Государственного бюджетного учреждения здравоохранения Пермского края «Ордена «Знак Почёта» Пермская краевая клиническая больница»

1. Общие положения и цели

1.1. ГБУЗ ПК «Пермская краевая клиническая больница» (далее – больница) является некоммерческой бюджетной организацией и осуществляет свою деятельность в соответствии с государственными заданиями учредителя, которые финансируются в виду субсидий из бюджета Пермского края. Деятельность больницы заключается в предоставлении медицинских услуг.

Осуществление данной деятельности подразумевает управление информацией, в том числе персональными данными, которые являются важным активом, и зависит от обеспечения информационной безопасности, под которой понимается обеспечение целостности, доступности и конфиденциальности информации.

1.2. Настоящая политика устанавливает цели, подходы и задачи информационной безопасности, которыми больница руководствуется в процессе своей деятельности.

1.3. Настоящая политика направлена на выполнение следующих целей:

a) Обеспечение непрерывности ведения бизнес-процессов;

b) Повышение имиджа и финансовой стабильности;

c) Минимизация возможных потерь и ущерба в случае нарушений в области информационной безопасности.

2. Описание объекта защиты

Объектами защиты системы информационной безопасности являются:

- Информационные ресурсы, содержащие врачебную тайну, персональные данные физических лиц, сведения ограниченного доступа, а также открыто распространяемая информация, необходимая для работы больницы;
- Сотрудники больницы, а также информация, прямо или косвенно относящаяся к ним, обрабатываемая в информационных системах;
- Информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;
- Информационная система обработки персональных данных.

3. Система управления информационной безопасностью

3.1. Для достижения указанных целей разработана система управления информационной безопасностью (далее – СУИБ), которая соответствует:

- требованиям законодательства РФ, нормативным и договорным обязательствам с точки зрения информационной безопасности;
- международному стандарту ISO/IEC 27001:2005;

3.2. СУИБ больницы задокументирована в настоящей Политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех сотрудников в области действия системы. Документированные требования СУИБ доводятся до сведения всех сотрудников больницы.

3.3. Руководство больницы обязано проводить мероприятия по контролю за состоянием СУИБ, её функционированием, а также проводить мероприятия по совершенствованию действующей СУИБ.

3.4. На предприятии обязан проводиться аудит информационной безопасности периодически или по случаю инцидента информационной безопасности. Аудит проводится уполномоченной аудиторской группой в установленные сроки.

3.5. Все информационные активы, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, персонал, подлежат обязательному учету в соответствии с их важностью и степенью доступа.

3.6. Для обеспечения физической защиты информационных активов больницы в пределах контролируемой зоны (больнично-поликлинический комплекс, расположенный по адресу: г. Пермь, ул. Пушкина, д. 85) устанавливаются зоны безопасности и принимаются меры для предотвращения несанкционированного доступа.

3.7. Информационно-вычислительный центр больницы обязан своевременно реагировать на все инциденты информационной безопасности, в соответствии с установленными правилами и процедурами, исправлять и совершенствовать СУИБ.

3.8. СУИБ предусматривает ролевую модель управления доступом на предприятии.

3.9. Сотрудники получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей. Больница проводит информирование, обучение и повышение квалификации работников в сфере информационной безопасности.

4. Аудит информационной безопасности

4.1. Аудит представляет собой независимую экспертизу отдельных областей функционирования СУИБ.

4.2. Аудит информационной безопасности производится периодически или по случаю инцидента информационной безопасности.

4.3. Аудит проводится для оценки эффективности системы внутреннего контроля Компании в области информационной безопасности. Оценка проводится по следующим направлениям:

- эффективность и результативность финансово-хозяйственной деятельности;
- сохранность активов;
- достоверность отчетности (внешней и внутренней);
- соответствие деятельности нормам законодательства, внутренним организационно-распорядительным документам и стандартам.

4.4. Аудит проводится уполномоченной аудиторской группой в установленные сроки.

4.5. Сотрудники службы внутреннего аудита уполномочены:

- запрашивать у должностных лиц и получать беспрепятственный доступ к любым активам, документам, бухгалтерским записям и другой информации о деятельности больницы, делать копии документов;
- в рамках выполнения аудиторских заданий проводить интервью с должностными лицами и сотрудниками;
- изучать и оценивать любые документы, запрашиваемые в ходе выполнения аудиторских заданий, и направлять копии этих документов и/или соответствующую информацию руководителю аудиторской группы;
- осуществлять мониторинг выполнения менеджментом мероприятий (корректирующих действий), осуществляемых по результатам проведенных аудитов;

- доводить до сведения руководителя аудиторской группы предложения по улучшению существующих систем, процессов, стандартов, методов ведения деятельности, а также комментарии по любым вопросам, входящим в компетенцию, как это определено в настоящем Положении.

4.6. По результатам аудита созывается заключительное совещание, с целью представить выводы по проведенному аудиту и принятию мер по устранению недостатков, если таковые имеются.

4.7. По результатам аудита разрабатываются отчетные документы, с указанием всех защитных мер.

5. Управление рисками информационной безопасности

5.1. В соответствии с настоящей Политикой осуществляется регулярная оценка рисков информационной безопасности. При ее проведении учитывается вероятность угроз информационной безопасности и степень их влияния на бизнес-процессы, финансовое состояние и репутацию больницы.

5.2. По результатам оценки рисков информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения информационной безопасности.

5.3. Оценка рисков производится по заданным таблицам воздействия (оценки актива) и вероятности инцидента ИБ.

6. Управление инцидентами информационной безопасности

6.1. Менеджмент инцидентов ИБ должен основываться на результатах мониторинга ИБ.

6.2. Основными целями менеджмента инцидентов ИБ являются:

- своевременное обнаружение инцидентов ИБ;
- адекватное и оперативное реагирование на них в интересах предотвращения реализации угроз ИБ;
- минимизация операционных рисков ИБ;
- минимизация и/или ликвидация негативных последствий для Компании (включая нарушение непрерывности банковских технологических процессов) при нарушениях ИБ.

6.3. Менеджмент инцидентов ИБ должен поддерживаться в Компании совокупностью нормативно-правовых, организационных и технических мер.

6.4. Для исключения и/или минимизации негативных последствий инцидентов ИБ на технологические процессы должна поддерживаться согласованность процедур менеджмента инцидентов ИБ с процедурами менеджмента рисков ИБ, процедурами управления операционными рисками, а также с процедурами по обеспечению непрерывности технологических процессов.

6.5. Работники больницы должны быть проинструктированы на основании материалов, подготавливаемых ответственным подразделением, о возможных инцидентах ИБ и относительно порядка действий в условиях их реализации.

6.6. Деятельность в рамках менеджмента инцидентов ИБ должна осуществляться как оперативный, непрерывный и автоматизированный процесс.

6.7. Сбор информации в процессе управления инцидентом ИБ, расследование причин возникновения инцидентов ИБ и выявление нарушителей ИБ, а также применение дисциплинарных и административных мер должны осуществляться с соблюдением законодательства РФ и договорных обязательств больницы.

7. Ответственность

7.1. Руководство больницы осуществляет общее управление информационной безопасностью и обеспечивает необходимые условия для:

- реализации мероприятий по оценке рисков информационной безопасности и защиты информации;
- поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
- регулярного обучения работников в сфере информационной безопасности.

7.2. Работники больницы несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности начальнику Информационно-вычислительного центра.

7.3. В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения своих обязанностей.

7.4. Ответственность работников больницы за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками больницы, а также положениями внутренних нормативных документов больницы.

8. Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности больницы осуществляется Начальником Информационно-вычислительного центра. Текущий контроль соблюдения настоящей Политики также осуществляет Информационно-вычислительный центр. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности больницы, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

9. Заключительные положения

9.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами больницы, которые дополняют и уточняют ее.

9.2. В случае изменения действующего законодательства и иных нормативных актов настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Информационно-вычислительный центр обязан незамедлительно инициировать внесение соответствующих изменений.

9.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

• периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 36 месяцев;

• внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности.

9.4. Ответственным за внесение изменений в настоящую Политику является Начальник Информационно-вычислительного центра.

9.5. Руководство больницы заявляет своё одобрение настоящей Политики, которая объявлена, распространена, внедрена и поддерживается на всех уровнях.

9.6. Политика информационной безопасности является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещается на официальном веб-сайте больницы.