Министерство здравоохранения Омской области
бюджетное учреждение здравоохранения Омской области
«КЛИНИЧЕСКИЙ ДИАГНОСТИЧЕСКИЙ ЦЕНТР»
(БУЗОО «КДЦ»)

ПРИКАЗ

26 января 2017 г. № 7 адм

г. Омск

Об организации работы по защите конфиденциальной информации и персональных данных

В целях организации работы по защите конфиденциальной информации и персональных данных в БУЗОО "КДЦ" в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 06 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера», постановления Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденного приказом Гостехкомиссии России от 30 августа 2002г. № 282, Федерального закона Российской Федерации от 21 ноября 2011г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие:

1.1. Политику информационной безопасности БУЗОО «КДЦ» (Приложение 1).

1.2. Описание технологического процесса обработки информации в информационных системах БУЗОО «КДЦ» (Приложение 2).

1.3. Порядок организации и проведения работ по защите информации в информационных системах БУЗОО «КДЦ» (Приложение 3).

1.4. Порядок учета средств защиты информации БУЗОО «КДЦ» (Приложение 4).

1.5. Форму журнала учета средств защиты информации БУЗОО «КДЦ» (Приложение 5).

1.6. Форму Журнала учета организационно-распорядительных документов по защите информации БУЗОО «КДЦ» (Приложение 6).

1.7. Перечень сведений конфиденциального характера (Приложение 7).

1.8. Положение о конфиденциальной информации (Приложение 8).

1.9. Форму Обязательства о неразглашении сведений конфиденциального

характера (Приложение 9).

1.10. Форму Журнала учета выдачи электронных идентификаторов (Приложение 10).

1.11. Порядок защиты информации от утечки по техническим каналам (Приложение 11).

1.12. Порядок организации парольной защиты в информационных системах БУЗОО «КДЦ» (Приложение 12).

1.13. Форму Парольной карты (Приложение 13).

1.14. Форма Журнала учета Парольных карт (Приложение 14).

1.15. Порядок проведения антивирусного контроля в информационных системах БУЗОО «КДЦ» (Приложение 15).

1.16. Форму Акта установки оборудования (Приложение 16).

1.17. Порядок технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационных систем БУЗОО «КДЦ» (Приложение 17).

1.18. План технического обслуживания средств вычислительной техники (Приложение 18).

1.19. Форму Журнала проверки исправности и технического обслуживания (Приложение 19).

1.20. Форму Заявки на внесение изменений в состав аппаратно-программных средств информационных систем (Приложение 20).

1.21. Форму Акта об удалении информации (остаточной), хранившейся на диске компьютера (Приложение 21).

1.22. Регламент резервного копирования информации (Приложение 22).

1.23. Перечень резервируемой информации (Приложение 23).

1.24. Регламент обеспечения защиты информационных ресурсов при удаленном доступе через сеть (Приложение 24).

1.25. Регламент по работе пользователей в информационных системах (Приложение 25).

1.26. Регламент администратора информационных систем (Приложение 26).

1.27. Регламент ответственного за обеспечение безопасности информации в информационных системах (Приложение 27).

1.28. Порядок организации работы с материальными носителями защищаемых информационных ресурсов (Приложение 28).

1.29. Порядок организации работы с электронными носителями конфиденциальной информации (Приложение 29).

2. Организовать работу с конфиденциальной информацией и персональными данными в БУЗОО "КДЦ", в соответствии с утвержденными регламентами, положениями, порядками.

3. Контроль за исполнением приказа оставляю за собой.

Главный врач Н.И. Орлова

Р.Х. Юсупов, 30-32-66

Приложение 1

к приказу от

26 января 2017 г. № 7 адм

ПОЛИТИКА

информационной безопасности БУЗОО "КДЦ"

1. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

ИБ – Информационная безопасность.

ИР – Информационные ресурсы.

ИС – Информационная система.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПДн – Персональные данные.

ПО – Программное обеспечение.

СЗИ – Средство защиты информации.

ЭВМ – Электронная – вычислительная машина, персональный компьютер.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов

утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений учреждения.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений БУЗОО "КДЦ" или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью БУЗОО "КДЦ" и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в БУЗОО "КДЦ" для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организации (штатный, временный и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети БУЗОО "КДЦ" и ПК.

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Вводные положения

2.1. Введение

Политика ИБ бюджетного учреждения здравоохранения Омской области "Клинический диагностический центр" (далее – БУЗОО "КДЦ", учреждение) определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется БУЗОО "КДЦ" в своей деятельности.

2.2. Цели

Основными целями политики ИБ являются защита информации БУЗОО "КДЦ" **от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы**

обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе БУЗОО "КДЦ".

Общее руководство обеспечением ИБ осуществляется главным врачом. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем учреждения несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов БУЗОО "КДЦ" по вопросам обеспечения ИБ.

2.3. Задачи

Политика ИБ направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба БУЗОО "КДЦ" обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне учреждения), либо иметь непреднамеренный ошибочный характер. Категории нарушителей и их возможности определяются в «Модели нарушителя».

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ в учреждении на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель

нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для БУЗОО "КДЦ". Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

– описание организации СУИБ;
– определение порядка сопровождения ИС БУЗОО "КДЦ";
– определение Политики ИБ, а именно: политика реализации антивирусной защиты; политика учетных записей; политика предоставления доступа к ИР; политика использования паролей; политика защиты АРМ; политика конфиденциального делопроизводства.

2.4. Область действия

Настоящая Политика распространяется на все структурные подразделения БУЗОО "КДЦ" и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

2.5. Период действия и порядок внесения изменений

Настоящая Политика вводится в действие и признается утратившей силу приказом главного врача.

Изменения в политику вносятся приказом главного врача БУЗОО "КДЦ".

Инициаторами внесения изменений в политику информационной безопасности являются:

– главный врач;
– заместители главного врача и руководители структурных подоазделений;

– администратор информационной безопасности.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ производится в обязательном порядке в следующих случаях:

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ учреждения;

– при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб учреждению;

– при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации.

Ответственность за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

3. Политика **информационной безопасности БУЗОО "КДЦ"**

3.1. Назначение политики информационной безопасности

Политика ИБ – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в БУЗОО "КДЦ".

Политика ИБ относится к административным мерам обеспечения ИБ и определяет стратегию учреждения в области ИБ.

Политика ИБ регламентирует эффективную работу СЗИ. Она охватывает все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика ИБ реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, должны быть утверждены главным врачом.

3.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства БУЗОО "КДЦ" с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ учреждения, корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей БУЗОО "КДЦ", а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3. Соответствие Политики безопасности действующему законодательству

Правовую основу политики составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

3.4. Ответственность за реализацию политики информационной безопасности

Ответственность за реализацию политики возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

– в части, касающейся доведения правил политики до сотрудников БУЗОО "КДЦ", а также иных лиц (см. область действия настоящей политики) – на АИБа;

– в части, касающейся исполнения правил политики, – на каждого сотрудника БУЗОО "КДЦ", согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

3.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация обучения сотрудников учреждения в области ИБ возлагается на АИБа. Обучение проводится согласно Плану, утвержденному главным врачом.

Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Допуск персонала к работе с защищаемыми ИР осуществляется только после ознакомления с настоящей политикой, а также после ознакомления пользователей с «Порядком работы пользователей», а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих документов подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ осуществляется после ознакомления с «Порядком организации работы с материальными носителями», «Порядком организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками БУЗОО "КДЦ", определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы БУЗОО "КДЦ"

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым приказом Главного врача.

4. Политики информационной безопасности

4.1.Политика предоставления доступа к информационному ресурсу

4.1.1.Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР учреждения.

4.1.2. Положение политики

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом приказом главного врача.

4.2. Политика учетных записей

4.2.1. Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов учреждения.

4.2.2. Положение политики

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов учреждения;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов учреждения назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

4.3. Политика использования паролей

4.3.1. Назначение

Настоящая Политика определяет основные правила парольной защиты в БУЗОО "КДЦ".

4.3.2. Положения политики

Положения политики закрепляются в «Порядке по организации парольной защиты».

4.4. Политика реализации антивирусной защиты

4.4.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в БУЗОО "КДЦ".

4.4.2. Положения политики

Положения политики закрепляются в «Порядке по проведению антивирусного контроля».

4.5. Политика защиты автоматизированного рабочего места

4.5.1. Назначение

Настоящая Политика определяет основные правила и требования по защите информации БУЗОО "КДЦ" от неавторизованного доступа, утраты или модификации.

4.5.2. Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

5. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в БУЗОО "КДЦ" и проведение разъяснительной работы по ИБ среди пользователей.

Положения определены документами, утвержденными Приказом «Об обучении сотрудников правилам защиты информации», и «Порядком технического обслуживания средств вычислительной техники».

5.1. Ликвидация последствий нарушения политик информационной безопасности

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать его указаниям.

Действия АИБа и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

– регламентом пользователя;
– политикой информационной безопасности;
– регламентом администратора информационной безопасности;
– регламентом системного администратора.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

5.2. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник БУЗОО "КДЦ" в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный учреждению в результате нарушения ими правил политики ИБ (ст. 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.