УТВЕРЖДАЮ

Главный врач ГБУЗ "КБ № 3"

_____Ф.В. Семенов

_____ 2016 года

ПОЛИТИКА
информационной безопасности в государственном бюджетом учреждении здравоохранения «Краевая больница № 3» министерства здравоохранения Краснодарского края (ГБУЗ «КБ № 3»)

1 Общие положения

Политика информационной безопасности ГБУЗ КБ № 3 (Далее - Учреждение) разработана с учетом требований федерального законодательства.

Политика информационной безопасности Учреждения определяет позицию руководства Учреждения в отношении информационной безопасности, основные цели, направления и меры обеспечения информационной безопасности, которыми Учреждение руководствуется в своей деятельности.

В рамках Политики, руководство Учреждения заявляет, что:

– информационные технологии входят в состав средств, используемых в реализации поставленных целей;

– информация является ценным ресурсом Учреждения, требующим защиты независимо от форм ее представления;

– в своей деятельности больницы сталкивается с широким спектром угроз информационной безопасности, как внутреннего, так и внешнего характера, реализация которых может привести к ущербу (финансовые потери, юридические взыскания, потеря репутации, дезорганизация и т.д.);

– стратегической целью больницы в области информационной безопасности является обеспечение функционирования и использования информационных технологий с учетом принимаемых рисков получения возможного ущерба от реализации угроз информационной безопасности;

Исполнение положений настоящей Политики информационной безопасности является обязательным для всех работников больницы.

1.1 Цели Политики информационной безопасности

Основными целями Политики информационной безопасности учреждения являются:

– обеспечение единых подходов к обеспечению информационной безопасности в рамках учреждения;

– создание методологической основы для разработки внутренних документов по информационной безопасности в учреждении;

– определение форм участия руководства учреждения в решении проблем информационной безопасности.

Основными целями процесса обеспечения информационной безопасности в учреждении являются:

– создание условий для устойчивого функционирования информационной инфраструктуры учреждения;

– поддержание необходимого уровня информационной безопасности в учреждении, соответствующего требованиям федерального законодательства.

1.2 Направления обеспечения информационной безопасности

Обеспечение информационной безопасности в учреждении осуществляется по следующим направлениям:

– управление информационной безопасности;

– идентификация и классификация объектов защиты;

– организация работы с персоналом по вопросам информационной безопасности;

– управление инцидентами информационной безопасности;

– обеспечение непрерывности бизнес-процессов;

– обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;

– обеспечение соответствия требованиям по информационной безопасности;

– обеспечение безопасности персональных данных сотрудников и пациентов учреждения.

Данные направления реализуются организационными и техническими мерами.

2 Управление информационной безопасностью

2.1 Внутренняя организация

Организация и обеспечение управления информационной безопасности в учреждении осуществляется его руководителем.

Руководство учреждения постоянно поддерживает необходимый уровень информационной безопасности путем внедрения системы обеспечения информационной безопасности, а также распределения обязанностей и ответственности работников больницы за ее внедрение и осуществление.

Организация плановой, непрерывной и целенаправленной работы по осуществлению мер обеспечения информационной безопасности и контролю их выполнения в Учреждении возлагается на ответственное лицо.

На ответственное лицо (структурное подразделение) по информационной безопасности возложены следующие функции:

– планирование работ по информационной безопасности;

– контроль эффективности реализуемых мер обеспечения информационной безопасности и внесение рекомендаций по их совершенствованию;

– координация действий по обеспечению информационной безопасности с представителями различных структурных подразделений учреждения;

– контроль выполнения и пересмотр политик информационной безопасности объектов защиты.

С учетом особенностей конкретных объектов информационной инфраструктуры в учреждении осуществляется:

– определение полномочий работников в отношении защищаемых информационных ресурсов;

– администрирование и контроль средств и механизмов безопасности;

– контроль выполнения работниками требований в области информационной безопасности.

Функции администрирования и контроля средств и механизмов безопасности в учреждении распределяются между ответственными лицами:

– администрирование встроенных механизмов безопасности средств обработки, хранения и передачи информации, а также дополнительных средств защиты осуществляется системным администратором и\или ответственным лицом (по договору по обслуживанию ИБ);

– контроль функционирования и настройки механизмов безопасности, а также соблюдения требований по информационной безопасности осуществляется системным администратором и\или ответственным лицом (по договору по обслуживанию ИБ).

В учреждении организуется администрирование информационной безопасности, направленное на обеспечение установленных правил доступа к объектам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении и передаче.

Администратором информационной безопасности назначается ответственное лицо и\или ответственным лицом (по договору по обслуживанию ИБ).

На администратора информационной безопасности возлагается ответственность по предотвращению несанкционированного доступа к защищаемой информации.

Обязанности работников учреждения по обеспечению информационной безопасности зависят от занимаемой должности и определяются их должностными инструкциями.

В каждом структурном подразделении назначается работник, ответственный за обеспечение информационной безопасности, перечень обязанностей которого разрабатывается с учетом специфики работы подразделения.

В учреждении ежегодно разрабатывается:

– план мероприятий по обеспечению информационной безопасности;

– план мероприятий по контролю состояния информационной безопасности.

2.2 Обеспечение информационной безопасности при работе с внешними организациями

При организации доступа сторонних организаций к защищаемым информационным ресурсам в учреждении осуществляются мероприятия по обеспечению информационной безопасности:

– определение рисков, связанных с предоставлением доступа сторонней организации к конфиденциальной информации;

– формирование на основе оценки рисков перечня мероприятий по обеспечению информационной безопасности при предоставлении доступа сторонней организации к конфиденциальной информации больницы и их реализация;

– заключение соглашения о конфиденциальности со сторонними организациями, которым предоставляется доступ к конфиденциальной информации больницы.

3 Идентификация и классификация объектов защиты

В целях обеспечения информационной безопасности в учреждении осуществляется идентификация объектов защиты информационной инфраструктуры, определение степени их критичности, классификация и назначение ответственных за их безопасную эксплуатацию.

4 Организация работы с персоналом по вопросам информационной безопасности

4.1 Обеспечение безопасности при заключении и во время действия трудового договора

В целях повышения уровня обеспечения информационной безопасности при приеме на работу новых работников осуществляется доведение до них правил обеспечения информационной безопасности и устанавливается ответственность за их нарушение.

Обязанности работников учреждения по соблюдению правил информационной безопасности определяются должностными инструкциями.

При приеме на работу учреждение заключает с работником соглашение о конфиденциальности.

В учреждении обеспечивается сохранность заключенных соглашений о конфиденциальности.

Все работники учреждения при вступлении в должность проходят первичный инструктаж, предусматривающий ознакомление с правилами и мерами информационной безопасности.

Для работников учреждения реализуются мероприятия повышения осведомленности в области информационной безопасности.

Работники, отвечающие за обеспечение информационной безопасности, регулярно проходят повышение квалификации, знакомятся с изменениями в федеральном законодательстве.

Работники учреждения, имеющие доступ к информации, подлежащей защите, несут ответственность за ее разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности.

Работники, разгласившие подлежащую защите информацию или нарушившие установленный порядок обращения с ней, а также работники, по вине которых

произошла ее утрата или искажение, несут ответственность в соответствии с действующим законодательством Российской Федерации.

4.2 Обеспечение безопасности при увольнении и при изменении условий трудового договора

В целях обеспечения информационной безопасности при увольнении и при изменении условий трудового договора в учреждении осуществляется контроль возврата технических средств обработки, хранения и передачи информации, своевременного прекращения прав доступа работников к объектам защиты учреждения.

Напоминание увольняемым работникам о принятых ими обязательствах по соблюдению в тайне конфиденциальных сведений и доведение до них срока сохранения в тайне сведений, с которыми они были ознакомлены, выполняются уполномоченным лицом.

В учреждении определяется порядок контроля возврата увольняемыми работниками взятых во временное пользование технических средств.

При увольнении работника (изменении условий трудового договора) его права доступа к информационным ресурсам незамедлительно аннулируются (приводятся в соответствие с новыми условиями).

5 Управление инцидентами информационной безопасности

5.1 Оповещение об инцидентах информационной безопасности

В целях предотвращения нарушений информационной безопасности, в учреждении принимаются меры по оповещению об инцидентах информационной безопасности.

Работники учреждения обязаны сообщать уполномоченному лицу о любых замеченных или предполагаемых нарушениях безопасности, а также выявленных уязвимостях в соответствии с установленным в больнице порядком.

5.2 Реагирование на инциденты информационной безопасности

В целях реагирования на инциденты информационной безопасности осуществляется их регистрация и анализ, а также принятие необходимых мер по исключению их повторения.

В учреждении назначаются работники, ответственные за реагирование на инциденты информационной безопасности, имеющие соответствующую подготовку.

6 Обеспечение непрерывности образовательного процесса

В целях обеспечения поддержки и восстановления образовательного процесса, осуществляются профилактические и восстановительные мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры больницы.

Состав мероприятий по обеспечению бесперебойного функционирования информационной инфраструктуры учреждения определяется с учетом оценки рисков информационной безопасности.

Мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры учреждения подвергаются тестированию и регулярному пересмотру.

7. Порядок обеспечения информационной безопасности на этапах жизненного цикла объектов информационной инфраструктуры

Информационная безопасность информационной инфраструктуры учреждения обеспечивается на всех стадиях жизненного цикла ее объектов с учетом ролей всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

Жизненный цикл объекта информационной инфраструктуры учреждения включает в себя следующие этапы:

- обоснование требований к объекту;
- разработка (модернизация) объекта;
- ввод объекта в действие;
- эксплуатация объекта;
- вывод объекта из эксплуатации.

Уполномоченное лицо учреждения в части сопровождения вопросов информационной безопасности участвует во всех этапах жизненного цикла объектов информационной инфраструктуры учреждения.

8. Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов

8.1 Физическая защита объектов информационной инфраструктуры

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры больницы обеспечивается физическая защита мест их эксплуатации (размещения).

Технические средства обработки, хранения и передачи информации размещаются в запираемых шкафах, располагаемых в специализированных помещениях, доступ посторонних лиц к которым ограничивается.

Порядок обеспечения физической защиты мест эксплуатации (размещения) объектов защиты определяется их политиками информационной безопасности.

8.2 Защита территорий, зданий и помещений

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений учреждения.

В учреждении устанавливается пропускной режим, препятствующий бесконтрольному посещению его охраняемых территорий и зданий. Порядок посещения и поведения в зданиях и помещениях учреждения регламентируется

нормативными и организационно-распорядительными документами учреждения в области информационной безопасности.

Здания и помещения учреждения обеспечиваются техническими средствами охраны, системами контроля доступа и пожарной безопасности.

При проведении работ на охраняемых территориях учреждения, в его зданиях и защищаемых помещениях третьими лицами обеспечивается контроль их деятельности.

8.3 Организация безопасной эксплуатации средств обработки, хранения и передачи информации

В целях обеспечения информационной безопасности объектов информационной инфраструктуры в учреждении устанавливаются правила безопасной эксплуатации средств обработки, хранения и передачи информации.

Принимаются меры по обеспечению использования средств обработки, хранения и передачи информации только по целевому назначению.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников.

8.4 Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения и нейтрализации вредоносного программного обеспечения в учреждении создается система защиты информационной инфраструктуры учреждения от вредоносного программного обеспечения.

В учреждении используются сертифицированные на соответствие требованиям безопасности информации средства защиты от вредоносного программного обеспечения. Архитектура системы защиты от вредоносного программного обеспечения обеспечивает многоуровневую (эшелонированную) защиту.

8.5 Обеспечение информационной безопасности при обращении со съемными носителями информации

В целях предотвращения разглашения, утечки или утраты информации в учреждении применяются меры защиты съемных носителей информации.

В учреждении разрешается применение только зарегистрированных установленным порядком съемных носителей информации.

Осуществляется мониторинг использования съемных носителей. Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

8.6 Защищенный обмен информацией

В целях предотвращения разглашения, утечки или утраты информации в учреждении применяются меры по защите информации при ее передаче различными методами.

8.7 Защита программного обеспечения

В целях поддержания работоспособности программного обеспечения в учреждении осуществляются меры по устранению уязвимостей программного обеспечения, а также другие меры защиты.

Устранение уязвимостей программного обеспечения достигается регулярным централизованным получением и установкой. Обновление программного обеспечения возлагается на системного администратора и\или ответственным лицом (по договору по обслуживанию ИБ).

8.8 Регистрация и учет событий информационной безопасности

В целях своевременного выявления нарушений информационной безопасности в учреждении осуществляется контроль событий информационной безопасности.

В учреждении осуществляется регистрация и учет в журналах событий технических средств обработки, хранения и передачи информации событий, которые могут быть связаны с нарушениями информационной безопасности. Журналы событий регулярно анализируются уполномоченным лицом, и\или ответственным лицом (по договору по обслуживанию ИБ). Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами информационной безопасности.

8.9 Контроль защищенности

В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости, а также устранения недостатков в конфигурации технических средств обработки, хранения и передачи информации в информационной инфраструктуре учреждения принимаются меры контроля защищенности.

Контроль защищенности осуществляется уполномоченным лицом, и\или ответственным лицом (по договору по обслуживанию ИБ). Перечень объектов контроля защищенности определяется по результатам идентификации и классификации объектов защиты.

8.10 Криптографическая защита

В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре учреждения применяются сертифицированные установленным порядком криптографические средства защиты.

Электронные документы, для которых необходимо обеспечить целостность и аутентичность защищаются с помощью электронной цифровой подписи.

При передаче информации ограниченного доступа вне контролируемых зон, в том числе при использовании беспроводных сетей, применяются средства криптографической защиты информации.

9 Контроль доступа

9.1 Управление доступом пользователей

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в больнице осуществляется управление доступом пользователей к ее информационным ресурсам, прикладным системам и соответствующим техническим средствам объектов защиты.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в больнице формализованной процедуре предоставления прав доступа. Целесообразно при этом использовать принцип ролевого управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

9.2 Ответственность пользователей

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации, определяется ответственность пользователей по соблюдению правил доступа при использовании автоматизированных рабочих мест (АРМ).

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям. При оставлении АРМ пользователями предпринимаются меры по защите их от несанкционированного доступа.

9.3 Контроль доступа к операционной системе

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры больницы осуществляется контроль доступа к операционной системе.

Работа пользователей в операционной системе осуществляется под учетными записями с ограниченными правами. Доступ к операционной системе предоставляется пользователям только после прохождения процедур идентификации и аутентификации.

Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также реализацией политики парольной защиты осуществляется системным администратором.

9.4 Контроль доступа к прикладным системам и информационным ресурсам

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования информационной инфраструктуры в учреждении обеспечивается контроль доступа к прикладным системам и информационным ресурсам.

Доступ к прикладным системам и информационным ресурсам предоставляется пользователям после прохождения ими процедур идентификации и аутентификации. При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и операционных системах.

9.5 Контроль доступа к сетевым сервисам

В целях предотвращения несанкционированного использования сетевых сервисов в информационной инфраструктуре учреждения осуществляется контроль доступа к сетевым сервисам.

Доступ к сетевым сервисам предоставляется пользователям объектов защиты только в виду служебной необходимости.

9.6 Контроль сетевого доступа

В целях предотвращения несанкционированного доступа в информационную инфраструктуру больницы и к ее информационным ресурсам в учреждении осуществляется контроль сетевого доступа.

Контроль сетевого доступа включает:

- контроль информационных потоков внешнего взаимодействия РСПД (ЛВС);
- контроль информационных потоков внешнего взаимодействия АСУ ТП;
- контроль внутренних информационных потоков ЛВС;
- контроль удаленного подключения к ЛВС.

9.7 Контроль доступа к сетевому оборудованию

В целях обеспечения безопасности сетевой инфраструктуры учреждения осуществляется управление доступом администраторов к сетевому оборудованию.

В информационной инфраструктуре учреждения обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования и сетевых средств защиты.

Доступ к управлению сетевым оборудованием и средствами защиты предоставляется только системному администратору и\или ответственным лицом (по договору по обслуживанию ИБ).

10 Обеспечение соответствия требованиям по информационной безопасности

10.1 Обеспечение соответствия правовым требованиям

В соответствии с законодательством Российской Федерации, требованиями нормативных и организационно-распорядительных документов больницы в области информационной безопасности в учреждении осуществляются меры по защите информации ограниченного доступа.

Защита информации ограниченного доступа в учреждении обеспечивается организацией:

- защиты персональных данных работников учреждения.

Допускается использование только официально приобретенного лицензионного программного обеспечения.

В составе объектов информационной инфраструктуры используются сертифицированные по требованиям безопасности информации или разрешенные к применению средства защиты информации.

Для защиты информации ограниченного доступа криптографическими методами в соответствии с законодательством Российской Федерации, используются сертифицированные по требованиям безопасности информации криптографические средства защиты.

10.1. Организация защиты персональных данных

В больнице устанавливается порядок защиты персональных данных работников, предусматривающий правовые, организационные и технические меры по их охране.

Перечень мер по защите персональных данных регламентируется Федеральным законом РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», Положением о защите персональных данных в ГБУЗ КБ № 3.

10.2 Обеспечение соответствия организационным и техническим требованиям

В целях предотвращения нарушений информационной безопасности осуществляется контроль выполнения требований нормативных и организационно-распорядительных документов больницы в области информационной безопасности.

К числу мер контроля относятся:

– регулярный контроль ответственным лицом выполнения требований информационной безопасности;

– внутренние проверки ответственным лицом и\или ответственным лицом (по договору по обслуживанию ИБ);

– анализ выявленных несоответствий и установление причин их возникновения;

– реализация корректирующих мер и устранение выявленных несоответствий.

10.3 Контроль состояния информационной безопасности

В целях определения соответствия принимаемых мер безопасности внутренним документам учреждения по информационной безопасности, выявления угроз информационной безопасности и принятия мер по противодействию им в учреждении осуществляется контроль состояния информационной безопасности.

Контроль состояния информационной безопасности осуществляется:

– проведением плановых (внеплановых) внешних проверок ответственным лицом (по договору по обслуживанию ИБ);

– проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом ответственным лицом.

Контроль состояния информационной безопасности осуществляется путем интервьюирования руководителей и работников, анализа документации, осуществления инструментальных проверок.

Результаты проведения контроля состояния информационной безопасности документируются.

11 Ответственность руководства и работников

Руководство учреждения отвечает за состояние информационной безопасности в учреждении и обеспечивает реализацию Политики информационной безопасности учреждения, включая регулярный контроль ее исполнения, актуализации и выделения необходимых для обеспечения информационной безопасности ресурсов, а также организацию осведомленности и обучения работников в области обеспечения информационной безопасности.

Ответственность за обеспечение информационной безопасности объектов защиты учреждения возлагается на работников, ответственных за их эксплуатацию.

Работники учреждения обязаны выполнять следующие общие требования по информационной безопасности:

– соблюдать требования настоящей Политики информационной безопасности и других нормативных и организационно-распорядительных документов Клиники в области информационной безопасности;

– использовать технические средства обработки информации только в служебных целях;

– осуществлять информирование уполномоченного лица о выявленных инцидентах информационной безопасности.

Работникам учреждения запрещается нарушать установленные правила обеспечения информационной безопасности и скрывать факты возникновения инцидентов информационной безопасности.

Работники учреждения, не выполняющие требования настоящей Политики информационной безопасности или требования нормативных и организационно-распорядительных документов учреждения в области информационной безопасности, могут быть привлечены к ответственности установленным порядком.

12 Порядок пересмотра Политики информационной безопасности

Политика информационной безопасности Общества пересматривается с периодичностью не реже чем 1 раз в 2 года. При пересмотре Политики информационной безопасности Учреждения учитываются результаты контроля эффективности обеспечения информационной безопасности за предыдущий период.

Процедура пересмотра Политики информационной безопасности учреждения включает:

– анализ и выявление несоответствий действующей Политики информационной безопасности учреждения текущим условиям;

– разработку предложений по совершенствованию Политики информационной безопасности учреждения;

– утверждение новой редакции Политики информационной безопасности учреждения.

При осуществлении процедуры пересмотра учитываются:

– результаты контроля состояния информационной безопасности и предложения работников о совершенствовании процедур обеспечения информационной безопасности;

– изменения в организационно-штатной структуре учреждения и в его информационной инфраструктуре;

– изменения в законодательной и нормативной базе по информационной безопасности, произошедшие с момента утверждения предыдущей Политики информационной безопасности учреждения;

– результаты анализа произошедших инцидентов информационной безопасности, а также уязвимости и угрозы, выявленные в учреждении за время, прошедшее с момента утверждения предыдущей Политики информационной безопасности учреждения;

– изменения в управлении информационной безопасности, включая изменения в распределении ресурсов и обязанностей при обеспечении информационной безопасности.