ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«НОВОСПАССКАЯ РАЙОННАЯ БОЛЬНИЦА»

УТВЕРЖДАЮ
Главный врач
ГУЗ «Новоспасская РБ»
_____ / К.В. Хомяков /
«___» _____ 2022 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

Вводные положения 3
1. Введение 3
2. Цели 3
3. Задачи 3
4. Область действия 4
5. Термины и определения 4
6. Обозначения и сокращения 7
7. Назначение политики информационной безопасности 7
8. Основные принципы обеспечения ИБ 7
9. Соответствие ПБ действующему законодательству 8
1). Ответственность за реализацию политик информационной безопасности 8
11. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе 8
12. Защищаемые информационные ресурсы ГУЗ «Новоспасская РБ» 8
13. Организация системы управления ИБ 9
14. Реализация системы управления ИБ 10
15. Методы оценивания информационных рисков 10
16. Политика предоставлениядоступакинформационномуресурсу 11
17. Политика защиты АРМ 11
18. Порядок сопровождения ИС ГУЗ «Новоспасская РБ» 11
19. Профилактика нарушений политик информационной безопасности 13
20. Ликвидация последствий нарушения политик информационной безопасности 13
21. Обязательства сотрудников 13
22. Ответственность нарушителей ПБ 13
23. Регулирующие законодательные нормативные документы 13

Вводные положения

1. Введение

Политика информационной безопасности ГУЗ «Новоспасская РБ» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ГУЗ «Новоспасская РБ» в своей деятельности.

2. Цели

Основными целями политики ИБ являются защита информации ГУЗ «Новоспасская РБ» и обеспечение эффективной работы при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ осуществляет главный врач ГУЗ «Новоспасская РБ». За организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несёт специалист информационной безопасности ГУЗ «Новоспасская РБ».

Руководители структурных подразделений ГУЗ «Новоспасская РБ» ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники ГУЗ «Новоспасская РБ» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

3. Задачи

Политика информационной безопасности 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 ГУЗ «Новоспасская РБ» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне ГУЗ «Новоспасская РБ»), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для ГУЗ «Новоспасская РБ». 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.

4, Область действия

Настоящая Политика распространяется на все структурные подразделения ГУЗ «Новоспасская РБ» 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.

5. Термины и определения

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

Анализ риска - систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности - процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим ГУЗ «Новоспасская РБ»м (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Доступ к информации - возможность получения информации и ее использования.

Защищенный канал передачи данных - логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами УРЫ), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа - уникальный признак субъекта или объекта доступа.

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 ГУЗ «Новоспасская РБ», имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность - механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов ГУЗ «Новоспасская РБ» 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 ГУЗ «Новоспасская РБ».

Информационная система - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ГУЗ «Новоспасская РБ». В ГУЗ «Новоспасская РБ» используются различные типы информационных систем для решения управленческих, учетных и других задач.

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

Информационные активы - информационные системы, информационные средства, информационные ресурсы.

Информационные средства - программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

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

Инцидент информационной безопасности - действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов ГУЗ «Новоспасская РБ».

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 ГУЗ «Новоспасская РБ», привести к причинению ГУЗ «Новоспасская РБ» материального или иного вида ущерба.

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

Мониторинг информационной безопасности - постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы ГУЗ «Новоспасская РБ», информационные услуги ГУЗ «Новоспасская РБ» и пр.

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска - процесс выбора и осуществления мер по модификации риска..

Остаточный риск — риск, остающийся после обработки риска.

Политика информационной безопасности - комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС — сотрудник ГУЗ «Новоспасская РБ» (штатный, временный, работающий по контракту 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.

Принятие риска - решение принять риск.

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. Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе ГУЗ «Новоспасская РБ» базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, Е-таП и т.п.

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

Средства криптографической защиты информации - средства шифрования, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным - 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.

Управление информационной безопасностью - совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта ГУЗ «Новоспасская РБ» (например, оценку и ГУЗ «Новоспасская РБ» рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость - недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности ГУЗ «Новоспасская РБ» 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.

ЭВМ- электронная - вычислительная машина, персональный компьютер.

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

6. Обозначения и сокращения

АРМ - Автоматизированное рабочее место.
АС - Автоматизированная система.
БД - База данных.
ЗИ - Защита информации.
ИБ - Информационная безопасность,.
ИС - Информационная система.
ИТС - Информационно-телекоммуникационная система.
КЗ - Контролируемая зона.
МЭ - Межсетевой экран.
НСД - Несанкционированный доступ.
ОС - Операционная система.
ПБ - Политики безопасности.
ПО - Программное обеспечение.
СВТ - Средства вычислительной техники.
СЗИ - Средство защиты информации.
СКЗИ - Средство криптографической защиты информации.
СПД - Система передачи данных.
СУБД - Система ГУЗ «Новоспасская РБ» базами данных.
СУИБ - Система ГУЗ «Новоспасская РБ» информационной безопасностью.
СЭД - Система электронного документооборота.
ЭВМ - Электронная - вычислительная машина, персональный компьютер.
ЭЦП - Электронная цифровая подпись.

7. Назначение политики информационной безопасности

Политики информационной безопасности ГУЗ «Новоспасская РБ» - это совокупность норм, правил и практических рекомендаций, на которых строится ГУЗ «Новоспасская РБ», защита и распределение информации в Управлении.

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию ГУЗ «Новоспасская РБ» в области ИБ.

Политики информационной безопасности (далее, ПБ) регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены главным врачом ГУЗ «Новоспасская РБ».

8. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

-Постоянный и всесторонний анализ информационного пространства ГУЗ «Новоспасская РБ» с целью выявления уязвимостей информационных активов.

-Своевременное обнаружение проблем, потенциально способных повлиять на ИБ ГУЗ «Новоспасская РБ», 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 ГУЗ «Новоспасская РБ», а также повышать трудоемкость технологических процессов обработки информации.

-Контроль эффективности принимаемых защитных мер.

-Персонификация и адекватное разделение ролей и ответственности между сотрудниками ГУЗ «Новоспасская РБ», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

9. Соответствие ПБ действующему законодательству

Правовую основу политик 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.

10. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт специалист по информационной безопасности ГУЗ «Новоспасская РБ».

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

Организация обучения сотрудников ГУЗ «Новоспасская РБ» в области информационной безопасности возлагается на специалиста по информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников ГУЗ «Новоспасская РБ» правилам обращения с конфиденциальной информацией, проводится путем:

-проведения инструктивных занятий с сотрудниками, принимаемыми на работу в ГУЗ «Новоспасская РБ»;

-самостоятельного изучения сотрудниками внутренних нормативных документов ГУЗ «Новоспасская РБ».

Допуск персонала к работе с защищаемыми информационными ресурсами ГУЗ «Новоспасская РБ» осуществляется только после его ознакомления с настоящими политиками, а так же иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

12. Защищаемые информационные ресурсы ГУЗ «Новоспасская РБ»

Различаются следующие категории информационных ресурсов, подлежащих защите в ГУЗ «Новоспасская РБ»:

Конфиденциальная - информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»,

постановлением правительства РФ от 17.11.2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная - информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая - информация, полученная от физических или юридических лиц, запрет на распространение И обработку которой был ими официально снят. Информация, сформированная в результате деятельности ГУЗ «Новоспасская РБ», которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности ГУЗ «Новоспасская РБ»;

Ограниченного доступа - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Подходы к решению проблемы защиты информации в Управлении, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов ГУЗ «Новоспасская РБ».

Для этого в Управлении выполняются следующие мероприятия:

-определяется порядок работы с документами, содержащими конфиденциальные сведения;

-устанавливается круг лиц и порядок доступа к подобной информации;

-вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

13. Организации системы управления ИБ

Система управления информационной безопасности ГУЗ «Новоспасская РБ» (СУИБ) - предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности ГУЗ «Новоспасская РБ».

Для успешного функционирования СУИБ ГУЗ «Новоспасская РБ» должны быть реализованы следующие процессы:

-определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

-определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью ГУЗ «Новоспасская РБ», а также оценки правовых рисков деятельности ГУЗ «Новоспасская РБ»;

-анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов.

-выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

-принятие руководством остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности ГУЗ «Новоспасская РБ», и оценено их влияние на достижение целей деятельности.

14. Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

-разработка плана обработки рисков ИБ;

-реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

-реализация программ по обучению и осведомленности ИБ;

-обнаружение и реагирование на инциденты безопасности;

-обеспечение непрерывности деятельности и восстановления после прерываний.

15. Методы оценивания информационных рисков

Оценка информационных рисков ГУЗ «Новоспасская РБ» выполняется по следующим основным этапам:

-идентификация и количественная оценка информационных ресурсов, значимых для работы ГУЗ «Новоспасская РБ»;

-оценивание возможных угроз;

-оценивание существующих уязвимостей:;

-оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые уязвимые информационные ресурсы ГУЗ «Новоспасская РБ» подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

-показателей ценности информационных ресурсов;

-вероятности реализации угроз для ресурсов;

-эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса ГУЗ «Новоспасская РБ».

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

-привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

-возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

-техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

-степенью легкости, с которой уязвимость может быть использована.

16. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам ГУЗ «Новоспасская РБ».

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику ГУЗ «Новоспасская РБ», допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Управлении одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

17. Политика защиты АРМ

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

18. Порядок сопровождения ИС ГУЗ «Новоспасская РБ»

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии специалиста по информационной безопасности.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

-неверной формулировки требований к ИС;

-выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;

-принятия неверных проектных решений;

-внесения разработчиком дефектов на уровне архитектурных решений;

-внесения разработчиком недокументированных возможностей в ИС;

-неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;

-разработки некачественной документации;

-сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

-неверного конфигурирования ИС;

-приемки ИС, не отвечающей требованиям заказчика;

-внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

-умышленное несанкционированное раскрытие, модификация или уничтожение информации;

-неумышленная модификация или уничтожение информации;

-недоставка или ошибочная доставка информации;

-отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

-внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

-невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб ГУЗ «Новоспасская РБ», и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

19. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Управлении и проведение разъяснительной работы по информационной безопасности среди пользователей.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

20. Ликвидация последствий нарушения политик информационной безопасности

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

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС необходимо уведомить главного врача, и далее следовать его указаниям.

21. Обязательства сотрудников

Каждый сотрудник ГУЗ «Новоспасская РБ» обязан :

- Не разглашать сведения, составляющие конфиденциальную информацию ГУЗ «Новоспасская РБ», которые будут доверены или станут известны по работе (службе);
- Не передавать третьим лицам и не раскрывать публично сведения, составляющие конфиденциальную информацию ГУЗ «Новоспасская РБ» без согласия ответственного лица;
- Выполнять относящиеся к своей работе требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информации ГУЗ «Новоспасская РБ»;
- В случае попытки посторонних лиц получить сведения о конфиденциальной информации ГУЗ «Новоспасская РБ» немедленно сообщить администратору информационной безопасности ГУЗ «Новоспасская РБ»;
- Не использовать знание конфиденциальной информации ГУЗ «Новоспасская РБ» для занятий любой деятельностью, которая может нанести ущерб ГУЗ «Новоспасская РБ»;
- В случае увольнения, все носители конфиденциальной информации ГУЗ «Новоспасская РБ», которые находились в распоряжении в связи с выполнением служебных обязанностей во время работы, незамедлительно передать администратору информационной безопасности ГУЗ «Новоспасская РБ»;
- Об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации ГУЗ «Новоспасская РБ», незамедлительно сообщать администратору информационной безопасности ГУЗ «Новоспасская РБ»;

22. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник ГУЗ «Новоспасская РБ» . Нарушение приказов, положений, регламентов, инструкций и прочих нормативно-правовых документов по ИБ может повлечь уголовную, административную, гражданско-правовую ответственность, в том числе и увольнение из ГУЗ «Новоспасская РБ» в соответствии с пп. в) п. 6 ст. 81 ТК РФ или иную ответственность, предусмотренную действующим законодательством Российской Федерации.

23. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники ГУЗ «Новоспасская РБ» должны руководствоваться следующими законодательными нормативными документами:

-Гражданский кодекс Российской Федерации;

-Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной цифровой подписи»;

-Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

-Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

-Уголовный кодекс РФ.