ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ТОМСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«МЕДИКО-САНИТАРНАЯ ЧАСТЬ № 2»

УТВЕРЖДАЮ
Главный врач
ОГБУЗ «Медико-санитарная часть №2»
_____ / А.В. Холопов /
«____» _____ 2021 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов ОГБУЗ «Медико-санитарная часть №2».

Информационная система - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ОГБУЗ «Медико-санитарная часть №2». В ОГБУЗ «Медико-санитарная часть №2» 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 ОГБУЗ «Медико-санитарная часть №2».

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 ОГБУЗ «Медико-санитарная часть №2», привести к причинению ОГБУЗ «Медико-санитарная часть №2» 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 ОГБУЗ «Медико-санитарная часть №2», информационные услуги ОГБУЗ «Медико-санитарная часть №2» 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.

-Своевременное обнаружение проблем, потенциально способных повлиять на ИБ ОГБУЗ «Медико-санитарная часть №2», 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 ОГБУЗ «Медико-санитарная часть №2», а также повышать трудоемкость технологических процессов обработки информации.

-Контроль эффективности принимаемых защитных мер.

-Персонификация и адекватное разделение ролей и ответственности между сотрудниками ОГБУЗ «Медико-санитарная часть №2», 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 инженер по защите информации ОГБУЗ «Медико-санитарная часть №2».

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

Организация обучения сотрудников ОГБУЗ «Медико-санитарная часть №2» в области информационной безопасности возлагается на специалиста по защите информации. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по защите информации». Обучение сотрудников ОГБУЗ «Медико-санитарная часть №2» правилам обращения с конфиденциальной информацией, проводится путем:

-проведения инструктивных занятий с сотрудниками, принимаемыми на работу в ОГБУЗ «Медико-санитарная часть №2»;

-самостоятельного изучения сотрудниками внутренних нормативных документов ОГБУЗ «Медико-санитарная часть №2».

Допуск персонала к работе с защищаемыми информационными ресурсами ОГБУЗ «Медико-санитарная часть №2» 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 защите информации».

12. Защищаемые информационные ресурсы ОГБУЗ «Медико-санитарная часть №2»

Различаются следующие категории информационных ресурсов, подлежащих защите в ОГБУЗ «Медико-санитарная часть №2»:

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 ОГБУЗ «Медико-санитарная часть №2», которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности ОГБУЗ «Медико-санитарная часть №2»;

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 ОГБУЗ «Медико-санитарная часть №2».

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 ОГБУЗ «Медико-санитарная часть №2» (СУИБ) - предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности ОГБУЗ «Медико-санитарная часть №2».

Для успешного функционирования СУИБ ОГБУЗ «Медико-санитарная часть №2» 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 ОГБУЗ «Медико-санитарная часть №2», а также оценки правовых рисков деятельности ОГБУЗ «Медико-санитарная часть №2»;

-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 ОГБУЗ «Медико-санитарная часть №2», 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 ОГБУЗ «Медико-санитарная часть №2» выполняется по следующим основным этапам:

-идентификация и количественная оценка информационных ресурсов, значимых для работы ОГБУЗ «Медико-санитарная часть №2»;

-оценивание возможных угроз;

-оценивание существующих уязвимостей:;

-оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые уязвимые информационные ресурсы ОГБУЗ «Медико-санитарная часть №2» 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 ОГБУЗ «Медико-санитарная часть №2».

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.

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 защите информации.

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.

информации ОГБУЗ «Медико-санитарная часть №2», незамедлительно сообщать администратору информационной безопасности ОГБУЗ «Медико-санитарная часть №2»;

22. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник ОГБУЗ «Медико-санитарная часть №2» . 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 ОГБУЗ «Медико-санитарная часть №2» 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 защите информации сотрудники ОГБУЗ «Медико-санитарная часть №2» 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.