Бюджетное учреждение Республики Калмыкия
«РЕСПУБЛИКАНСКИЙ ДЕТСКИЙ МЕДИЦИНСКИЙ ЦЕНТР
ИМЕНИ МАНДЖИЕВОЙ ВАЛЕНТИНЫ ДЖАЛОВНЫ»

ПРИКАЗ

«06» февраля 2024г. Элиста № 125

«Об утверждении модели угроз информационной безопасности»

С целью обеспечения безопасности и повышению защищенности объектов критической информационной инфраструктуры (далее-КИИ),

приказываю:

1. Утвердить модель угроз информационной безопасности в соответствии с приложением № 1 к настоящему приказу.
2. Назначить ответственными лицами за:
   2.1. обеспечение безопасности объектов КИИ администратора безопасности: программиста Сельдикова Баира Павловича (на период его отсутствия – техников-программистов Максимова Сергея Леонидовича и Пюрбеева Санджа Владимировича).
   2.2. осуществление контроля обеспечения безопасности объектов КИИ заместителя главного врача по ОМР Джанджиеву А.И.
3. Ответственным лицам:
   - по п.2.1. обеспечить безопасность и провести работу по повышению защищенности объектов КИИ в подразделениях БУ РК «РДМЦ им. Манджиевой В.Д.» (периодически проводить внеплановые смены паролей привилегированных пользователей, реализацию для них двухфакторной аутентификации; проведение инструктажа о недопущении передачи сторонним лицам своей идентификационной и (или) аутентификационной информации (учетных данных, паролей, токенов); информирование об административной, уголовной и иных видах ответственности за нарушение требований по обеспечению безопасности объектов критической информационной инфраструктуры);
4. Начальнику отдела кадров Хундаии Ю.Ю. ознакомить ответственных лиц: заместителя главного врача по ОМР Джанджиеву А.И., программиста Сельдикова Б.П., техников-программистов Максимова С.Л. и Пюрбеева С.В. путем направления сканкопии приказа электронно.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Дорджиев А.Н.

Модель угроз
медицинской информационной системы «Самсон»
(МИС «Самсон»)
БУ РК «Республиканский детский медицинский центр имени Манджиевой Валентины Джаловны»

СОДЕРЖАНИЕ

Сокращения

АС – автоматизированная система

АРМ – автоматизированное рабочее место

БД – база данных

ИКХ – информация конфиденциального характера

ИСПДн – Информационная система персональных данных

ЛВС – локальная вычислительная сеть

ЛПУ – Лечебно- профилактическое учреждение

НСД – несанкционированный доступ к информации

ПДн – Персональные данные

ППО – Прикладное программное обеспечение

СЗПДн – Система защиты персональных данных

СВТ – средства вычислительной техники

СЗИ – средство защиты информации

СФ – среда функционирования

ФСТЭК – Федеральная служба по техническому и экспортному контролю России

HL7 – Международный медицинский стандарт

Термины и определения

В настоящем документе используются следующие термины и их определения:

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Доверенное лицо - лицо, которое уполномочили действовать от имени доверителя, нанимателя.

Информационные ресурсы - (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.).

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Лечебно-профилактическое учреждение (ЛПУ) – БУ РК «РДМЦ им. Манджиевой В.Д.» - многопрофильный детский центр, предназначенный для оказания первичной медико-санитарной, специализированной, в том числе высокотехнологичной, медицинской помощи детскому населению Республики Калмыкия.

1 Введение

Настоящий документ подготовлен в рамках выполнения работ по построению системы защиты персональных данных (далее – СЗПДн), не содержащей сведений, составляющих государственную тайну, медицинской информационной системы «Самсон» (далее – МИС).

Настоящий документ содержит модель угроз для МИС (далее – модель угроз).

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации МИС и проектирования СЗПДн МИС.

Модель угроз – документ, использующийся для:

анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

контроля обеспечения уровня защищенности персональных данных.

Модель угроз для ИСПДн МИС разрабатывается в соответствии со следующими нормативными и методологическими документами:

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

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

- Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Приказ ФСТЭК России от 18.02.2013г № 21 (в ред. от 14.05.2020г.) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В процессе развития МИС предполагается конкретизировать и пересматривать модель угроз для МИС.

При разработке модели угроз для МИС учитывается:

1. МИС является специальной информационной системой так как, в ней обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

2. в МИС одновременно обрабатываются данные более 1000 субъектов персональных данных;

3. в МИС не предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных (юридически значимым документом является «бумажная» история болезни, по которой принимаются решения).

2 Назначение, структура и основные характеристики МИС

Медицинская информационная система «Самсон» (далее-МИС) предназначена для поддержки технологических процессов работы БУ РК «РДМЦ им. Манджиевой В.Д.» (далее – ЛПУ).

Медицинская информационная система позволяет вести полный учет оказанных пациенту медицинских услуг, автоматически формирует необходимую медицинскую документацию (первичный осмотр, дневники, протоколы дополнительных исследований, выписки, стандартные бланки для ЛПУ), составляет подробные отчеты о работе ЛПУ и персонала по установленным статистическим и произвольным формам.

МИС не имеет подключения к сетям общего пользования и (или) международного обмена и другим информационным системам.

Все компоненты МИС находятся внутри контролируемой зоны.

МИС, будучи комплексным решением, состоит из модулей и опций к этим модулям. Каждый модуль содержит определенную функциональность, которая позволяет ЛПУ автоматизировать определенные виды своей деятельности. Каждая опция относится к одному из модулей и содержит дополнительную функциональность, отсутствующую в базовой поставке модуля.

Основные модули, присущие МИС:

ЭЛЕКТРОННАЯ МЕДИЦИНСКАЯ КАРТА

В БУ РК «РДМЦ им. Манджиевой В.Д.» используется амбулаторная карта и история болезни пациента в электронном виде. Экспорт ЭМК во внешний формат.

СТАТИСТИКА

Автоматизация медицинской статистики и других форм отчетности.

Оперативный доступ к отчетам разного вида: управленческим, финансовым, медицинской статистики, материального учета. Возможность создания отчетов любой сложности.

РАСПИСАНИЕ

Поддержка расписания приема врачей, диагностических кабинетов.

ЛАБОРАТОРИЯ

Лабораторный модуль для организации процесса лаборатории и работа по направлениям. Поддерживаются лабораторные профили с возможностью ввода или автоматизированного импорта результатов исследований от анализаторов.

УЧЕТ УСЛУГ

Учет медицинских услуг и взаиморасчеты с различными контрагентами медицинских учреждений – страховыми компаниями, предприятиями и пациентами.

КАССА

Интеграция с фискальным регистратором для реализации рабочего места кассира. Интеграция с бухгалтерской системой, возможность экспорта документов и проводок в бухгалтерскую программу ЛПУ.

АПТЕКА

Поддержка складов медикаментов и расходных материалов. Ведется персонифицированный учет расхода при оказании медицинских услуг.

КОЕЧНЫЙ ФОНД

Для ЛПУ в МИС предусмотрен модуль планирования и учета палатного и коечного фонда.

ПЛАНЫ ЛЕЧЕНИЯ

План лечения – механизм поддержки стандартов лечения в единстве и взаимодействии с другими модулями МИС и удобное средство, облегчающее работу врача.

СТАНДАРТЫ ЛЕЧЕНИЯ

Использование государственных стандартов лечения с помощью общего механизма работы с планами лечения и справочника шаблонов.

РЕПЛИКАЦИЯ

МИС обеспечивает возможность обмена электронными медицинскими картами между разными учреждениями, синхронизации справочников и консолидации финансовой информации.

ОБРАБОТКА ИЗОБРАЖЕНИЙ

Получение и хранение медицинских изображений в современных условиях обеспечивают, как правило, специализированные комплексы оборудования и программных средств. В МИС могут быть предусмотрены механизмы для организации структурированного хранилища изображений, поиска, просмотра и редактирования изображений.

МОДУЛЬ СОПРЯЖЕНИЯ

Обеспечивает подключение медицинского оборудования и организация импорт данных из внешних источников с помощью оригинальных технологий обмена информацией.

СИСТЕМНОЕ ЯДРО

Обеспечение безопасности и конфиденциальности данных является одним из ключевых требований к современной МИС. Обеспечивает доступ к базе данных и реализует систему безопасности в работе с данными. Включает в себя модуль статистики.

МИС должна обеспечивать выполнение следующих функций:

- Регистратура и расписание приема
- Учет оказанных услуг
- Электронная история болезни / электронная медицинская карта
- Расчеты с пациентами, страховыми компаниями и подрядчиками
- Медико-экономические стандарты
- Статистика и аналитика
- Автоматизация стационара

- Управление сетью филиалов
- Ведение БД пациентов, врачебного и сестринского персонала
- (Учет работы служб неотложной помощи и оказания помощи на дому)

Для обеспечения удобства работы медицинского персонала программы МИС ЛПУ имеют возможность объединения функций на одном АРМе.

Предусмотрена возможность параметрической адаптации программ под особенности ЛПУ.

При своем функционировании система решает следующие задачи:

- Поиск и регистрация пациентов;
- Запись на прием;
- Ведение электронной истории болезни;
- Ввод результатов проведенных лабораторных и специальных исследований;
- Формирование и печать медицинских документов;
- Ограничение доступа оператора в прикладную программу;
- Ведение журнала учета работы операторов на каждом автоматизированном рабочем месте (АРМ);
- Регистрация изменений в БД и ведение фискальной БД;
- Ведение аптечного учета (для стационара);
- Ведение продовольственного учета (для стационара);
- Формирование обобщенных отчетов по текущей деятельности ЛПУ.

Серверное оборудование и АРМ медицинского персонала объединены в локальную вычислительную сеть и обеспечивают надежную работу информационной системы.

Для функционирования прикладных программ в состав МИС входит следующее специальное оборудование:

- Лазерные, струйные и матричные принтеры с подключением к LPT или USB разъему системного блока;

В МИС обрабатываются следующие типы ПДн:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес проживания, адрес регистрации;
- паспортные данные, данные свидетельства о рождении;
- данные СНИЛС;
- данные медицинского полиса;
- медицинская информация.

Работа в ИСПДн МИС ведется в многопользовательском режиме с разграничением прав доступа.

- Разграничение доступа обеспечивается за счет идентификации субъектов. При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей МИС. МИС располагает необходимыми данными для идентификации, аутентификации, а также препятствует несанкционированному доступу к ресурсам.

3 Модель вероятного нарушителя информационной безопасности:

3.1 Описание возможных нарушителей

По признаку принадлежности к МИС все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование МИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование МИС.

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в МИС, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования МИС, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам МИС в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы МИС (категория I);
- администраторы конкретных подсистем или баз данных МИС (категория II);
- пользователи МИС (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);

- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам (категория VI);
- обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.) (категория VII);
- уполномоченный персонал разработчиков МИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов МИС (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных МИС для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав МИС. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в МИС, а также к техническим и программным средствам МИС, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и МИС в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в МИС должен применяться комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

3.2 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- информации о назначения и общих характеристиках МИС;
- информация, полученная из эксплуатационной документации;
- информация, дополняющая эксплуатационную информацию об МИС (например, сведения из проектной документации МИС).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах МИС;
- сведения об информационных ресурсах МИС: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств МИС;
- данные о реализованных в ПСЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения МИС;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об МИС и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств МИС. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам МИС в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания необходимых условий безопасности персональных данных предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

3.3 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

3.4 Описание объектов и целей реализации угроз информационной безопасности

Основными информационными ресурсами, обрабатываемыми в МИС являются следующие:

1. Целевая информация:

- служебная информация;
- персональные данные сотрудников;
- сведения из БД МИС;
- другие виды информации конфиденциального характера.

2. Технологическая информация:

- защищаемая управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- защищаемая технологическая информация средств доступа к системам управления МИС (аутентификационная информация и др.);
- информационные ресурсы МИС на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами МИС (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
- информация о СЗПДн, их структуре, принципах и технических решениях защиты;
- информационные ресурсы МИС (базы данных и файлы), содержащие информацию о информационно телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах.

3. Программное обеспечение:

- программные информационные ресурсы МИС, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами МИС, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств защиты.

Предполагается, что не являются объектами реализации угроз:

- технические каналы утечки информации;
- сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- источники и цепи электропитания;
- цепи заземления.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

3.5 Описание каналов реализации угроз информационной безопасности

Возможными каналами реализации угроз информационной безопасности являются:

– каналы доступа, образованные с использованием штатных средств МИС.

– каналы доступа, образованные с использованием специально разработанных технических средств и программного обеспечения.

Предполагается, что не являются каналами реализации угроз:

- технические каналы утечки;
- сигнальные цепи;
- источники и цепи электропитания;
- цепи заземления;
- каналы активного воздействия на технические средства с помощью облучения.

3.6 Основные способы реализации угроз информационной безопасности

При определении основных способов реализации угроз информационной безопасности ресурсов МИС, учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла МИС, компонентов, условий функционирования МИС, а также – предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности МИС:

1) несанкционированный доступ к защищаемой информации с использованием штатных средств МИС и недостатков механизмов разграничения доступа;
2) негативные воздействия на программно-технические компоненты МИС вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;
3) маскировка под администратора МИС, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых МИС;
4) осуществление прямого хищения (утраты) элементов МИС, носителей информации и производственных отходов (распечаток, списанных носителей);
5) компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых МИС;
6) методы социальной инженерии для получения сведений об МИС, способствующих созданию благоприятных условий для применения других методов;
7) использование оставленных без присмотра незаблокированных средств администрирования МИС и АРМ;
8) сбои и отказы программно-технических компонентов МИС;
9) внесение неисправностей, уничтожение технических и программно-технических компонентов МИС путем непосредственного физического воздействия;
10) осуществление несанкционированного доступа к информации при ее передаче.

4 Перечень основных угроз безопасности информации

При разработке описаний угроз учитывались:

- основные характеристики МИС;
- ресурсы МИС, потенциально подверженные угрозам информационной безопасности;
- основные каналы реализации угроз информационной безопасности;
- основные способы реализации угроз информационной безопасности.

Разработанные описания угроз информационной безопасности изложены в следующей структуре:

- аннотация угрозы;
- возможные источники угрозы;
- способ реализации угрозы;
- используемые уязвимости;
- вид ресурсов, потенциально подверженных угрозе;
- нарушаемые характеристики безопасности ресурсов;
- возможные последствия реализации угрозы.

К основным угрозам безопасности информации МИС относятся следующие:

Угроза 1

1. Аннотация угрозы – осуществление несанкционированного ознакомления, модификации и блокировки целевой информации, хранимой и обрабатываемой в МИС.

2. Возможные источники угрозы:

1) пользователи МИС;

2) сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам;

3) обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.);

4) лица, обладающие возможностью доступа к системе передачи данных;

5) пользователи, являющиеся внешними по отношению к конкретной АС.

3. Способы реализации угрозы:

1) осуществление несанкционированного доступа, используя штатные средства МИС;

2) использование бесконтрольно оставленных технических средств;

3) хищение нарушителями и утрата уполномоченными лицами технических средств МИС (в том числе носителей информации);

4) несанкционированный просмотр средств отображения информации и распечатанных документов.

4. Используемые уязвимости – недостатки механизмов разграничения доступа и организационных мероприятий, связанные с возможностью осуществления несанкционированного доступа к защищаемой информации.

5. Вид ресурсов, потенциально подверженных угрозе – целевая информация.

6. Нарушаемые характеристики безопасности ресурсов – конфиденциальность, целостность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с защищаемой информацией; искажение информации; непредставление целевой информации потребителям в отведенные временные рамки.

Угроза 2

1. Аннотация угрозы – осуществление несанкционированного ознакомления с конфигурационными файлами и настройками средств защиты информации.

2. Возможные источники угрозы:

1) пользователи МИС;

2) сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам;

3) обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.);

4) уполномоченный персонал разработчиков МИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов МИС;

5) пользователи, являющиеся внешними по отношению к конкретной АС.

3. Способы реализации угрозы:

1) маскировка под администраторов МИС, уполномоченных на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых МИС;

2) осуществление прямого хищения элементов МИС, носителей информации и производственных отходов (распечаток, списанных носителей);

осуществление несанкционированного визуального просмотра защищаемой технологической информации, отображаемой на средствах отображения (экранах мониторов), несанкционированного ознакомления с распечатываемыми документами, содержащими технологическую информацию

4. Используемые уязвимости:

1) недостатки механизмов разграничения доступа, связанные с возможностью маскировки под уполномоченного администратора МИС;

2) недостатки мер физической защиты, связанные с возможностью хищения элементов МИС, носителей информации, производственных отходов и последующего их несанкционированного анализа;

недостатки реализации необходимых организационных мероприятий на объектах МИС, связанные с возможностью несанкционированного визуального просмотра технологической информации на средствах отображения (экранах мониторов), а так же несанкционированного ознакомления с распечатываемыми документами, содержащими защищаемую информацию.

5. Вид ресурсов, потенциально подверженных угрозе – защищаемая технологическая (управляющая) информация.

6. Нарушаемые характеристики безопасности ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с защищаемой информацией; подготовка к осуществлению несанкционированных действий, в том числе, направленных на снижение уровня защищенности МИС.

Угроза 3

1. Аннотация угрозы – осуществление несанкционированной модификации конфигурационных файлов и настроек средств защиты информации.

2. Возможные источники угрозы:

1) пользователи МИС;

2) сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам;

3) обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.);

4) пользователи, являющиеся внешними по отношению к конкретной АС.

3. Способы реализации угрозы:

1) маскировка под администратора МИС, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых МИС;

2) компрометация (просмотр, подбор и т.п.) аутентификационной (парольной) информации на доступ к информационным ресурсам МИС с

3). использованием штатных средств, предоставляемых МИС, а также используя методы социальной инженерии;

4). осуществление доступа к конфигурационным файлам и настройкам средств защиты, используя оставленные без присмотра незаблокированные средства администрирования МИС.

4. Используемые уязвимости:

1) недостатки механизмов разграничения доступа, связанные с возможностью маскировки под уполномоченного администратора МИС;

2) недостатки механизмов защиты технологической (аутентификационной) информации от возможности ее компрометации;

3) недостатки реализации необходимых организационных мероприятий и технических мер защиты на объектах МИС, связанные с возможностью несанкционированного доступа к оставленным без присмотра средствам администрирования МИС.

5. Вид ресурсов, потенциально подверженных угрозе – защищаемая управляющая информация.

6. Нарушаемые характеристики безопасности ресурсов – целостность.

7. Возможные последствия реализации угрозы – несанкционированное модификация (подмена) защищаемой информации; осуществление и способствование осуществлению несанкционированных действий, в том числе, направленных на снижение уровня защищенности МИС.

Угроза 4

1. Аннотация угрозы – нарушение режимов функционирования программно-технических средств МИС.

2. Возможные источники угрозы:

1) пользователи МИС;

уполномоченный персонал разработчиков МИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов МИС;

1) сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам;

2) обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.);

3) лица, обладающие возможностью доступа к системе передачи данных.

3. Способы реализации угрозы:

1) внедрение на АРМ и сервера МИС компьютерных вирусов или другого вредоносного программного обеспечения;

2) осуществление сбоев и отказов, внесение неисправностей, уничтожение технических и программно-технических компонентов МИС путем непосредственного воздействия.

4. Используемые уязвимости:

1) недостатки механизмов защиты МИС от внедрения компьютерных вирусов или другого вредоносного программного обеспечения;

2) недостатки механизмов физической защиты, резервирования компонентов МИС, связанные с возможностью осуществления сбоев, внесения неисправностей, уничтожения технических и программнотехнических компонентов МИС.

5. **Вид ресурсов, потенциально подверженных угрозе –** программное обеспечение.

6. **Нарушаемые характеристики безопасности ресурсов –** целостность.

7. **Возможные последствия реализации угрозы –** сбои и отказы программно-технических компонентов МИС; нарушение работоспособности МИС.

5. Выводы

1. Ввиду исключительной роли в МИС лиц категорий I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

2. Лица категорий III-VIII относятся к вероятным внутренним нарушителям.

3. Среди лиц категорий III-VIII наиболее опасными вероятными нарушителями являются лица категории III (пользователи МИС) и лица категории VIII (уполномоченный персонал разработчиков МИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов МИС).

4. Лица категории III и лица категории VIII в качестве вероятных нарушителей безопасности информации МИС обладают возможностями, соответствующими нарушителю второго уровня (в соответствии с руководящим документом ФСТЭК России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»).

5. Представленная модель угроз для МИС должна использоваться при формировании обоснованных требований информационной безопасности МИС и проектировании СЗПДн ЛПУ.

6. Исходя из анализа угроз безопасности ПДн, а так же учитывая то, что:

– МИС является специальной информационной системой т.к., в ней обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

– в МИС одновременно обрабатываются данные более 1000 субъектов персональных данных;

- в МИС не предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных (юридически значимым документом является «бумажная» история болезни, по которой принимаются решения);

- нарушение безопасности персональных данных, обрабатываемых в МИС, может привести к незначительным негативным последствиям для субъектов персональных данных;

- класс информационной системы определяется по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных.

Учитывая особенности функционирования, небольшое количество актуальных угроз и незначительность опасности их реализации, МИС определяется как специальная ИСПДн с требованиями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в основном, соответствующими 3-му классу.