Министерство образования и науки Кыргызской Республики

Кыргызский государственный технический университет им. И.Раззакова

Факультет информационных технологий

Кафедра «Программное обеспечение компьютерных систем»

Отчет

**На тему: «Информационная система урологического центра»**

Студенты группы ИБ(б)-1-17: Мажитов Кенешбек Абдибахапович

Бишкек 2021

Оглавление

[Цель: 3](#_Toc64902776)

[Решаемые задачи 3](#_Toc64902777)

[Термины и определения: 4](#_Toc64902778)

[Обозначение и сокращения 6](#_Toc64902779)

[Введение: 6](#_Toc64902780)

[Аналитическая часть: 7](#_Toc64902781)

[Общая характеристика объекта защиты или исследования: 7](#_Toc64902782)

[Обзор и анализ существующих систем 7](#_Toc64902783)

[Описание системы: 10](#_Toc64902784)

[Концептуальная модель 11](#_Toc64902785)

[Контекстная диаграмма AS-IS 13](#_Toc64902786)

[Контекстная диаграмма TO-BE 14](#_Toc64902787)

[Основные процессы и информационные потоки: 14](#_Toc64902788)

[Модель потоков данных 15](#_Toc64902789)

[Теоретическая часть 17](#_Toc64902790)

[Идентификация активов: 17](#_Toc64902791)

[Модели информационной безопасности: 20](#_Toc64902792)

[Модель угроз ИБ урологического центра: 20](#_Toc64902793)

[Модель нарушителя ИБ урологического центра: 21](#_Toc64902794)

[Политика ИБ урологического центра 27](#_Toc64902795)

[Структура Политики ИБ урологического центра 27](#_Toc64902796)

[Общие сведения о Политике ИБ АИС Урологического центра 28](#_Toc64902797)

[Субъекты Политики ИБ 28](#_Toc64902798)

[Пересмотр Политики ИБ 29](#_Toc64902799)

[Проектная часть 29](#_Toc64902800)

[Актуальность угроз ИБ: 29](#_Toc64902801)

[Политика безопасности ИБ ИС Урологического центра 38](#_Toc64902802)

[Введение 38](#_Toc64902803)

[Цели и задачи политики ИБ 38](#_Toc64902804)

[Область действия 38](#_Toc64902805)

[Описание активов, подлежащих защите 38](#_Toc64902806)

[Угрозы ИБ 40](#_Toc64902807)

[Требования и правила 41](#_Toc64902808)

[Субъекты Политики ИБ 42](#_Toc64902809)

[Повышение осведомленности в области ИБ 42](#_Toc64902810)

[Контроль реализации Политики ИБ 42](#_Toc64902811)

[Пересмотр Политики ИБ 42](#_Toc64902812)

[Модель угроз ИБ ИС Урологического центра 43](#_Toc64902813)

[Модель нарушителей ИБ ИС Урологического центра 51](#_Toc64902814)

# Цель:

Целью данной работы является изучение информационной системы частного урологического центра, обеспечение безопасности этой системы.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

Общая характеристика объекта защиты или исследования:

Частная урологическая клиника

# Термины и определения:

|  |  |  |
| --- | --- | --- |
| **Актив** | – | все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении [1].  Дополнительно:  К активам организации могут относиться:  активы информационные, в том числе различные виды информации, циркулирующие в системе информационной (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);  ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);  процессы (технологические, информационные и пр.);  выпускаемая продукция и/или оказываемые услуги. |
| **Доступность информации** | – | состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут беспрепятственно их реализовывать [2].  Дополнительно:  К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов. |
| **Защита информации** | – | защита конфиденциальности, целостности и доступности информации [3]. |
| **Информация** | – | сведения (сообщения, данные) независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на информацию общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [4]. |
| **Информационная безопасность** | – | состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность [5]. |
| **Конфиденциальность** | – | свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса [6]. |
| **Целостность информации** | – | состояние защищенности информации, характеризуемое способностью информационной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения [7]. |

# Обозначение и сокращения

|  |  |  |
| --- | --- | --- |
| ЭМК | – | электронная медицинская карта |
| БД | – | база данных. |
| ИА | – | информационный актив. |
| ИБ | – | информационная безопасность. |
| НСД | – | несанкционированный доступ. |
| ОС | – | операционная система. |
| ПК | – | персональный компьютер. |
| ПО | – | программное обеспечение. |
| СУБД | – | система управления базой данных. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Введение:

В настоящее время сфера здравоохранения использует информационные системы для улучшения качества работы своих специалистов. Во многие больницы, поликлиники и медицинские центры вводятся информационные системы.

Сфера здравоохранения пытается облегчить работу для своих сотрудников. Компьютерные информационные технологии находят все большее применение в медицинской деятельности. Если раньше вся работа проходила на бумагах, которые хранились в пыльных архивах. То сейчас по большей части она проходит на компьютерах.

У каждого медицинского учреждения есть свой архив, в котором хранятся данные о их пациентах. Их медицинские карты с диагнозами и анализами. Не каждый пациент захочет, чтобы их личные данные стали известны посторонним лицам. Поэтому, такая информация должна быть должным образом защищена.

К большому сожалению, сотрудники в медицинских центрах не обучены правильному использованию таких систем. В связи с этим происходит множество утечек важных данных.

Тема данной работы актуальна, поскольку в настоящее время всё большую популярность получают компьютерные информационные системы, облегчающие работу сотрудников различных сфер деятельности, а также позволяющие быстро и качественно предоставить необходимую информацию.

Правильная организации работы сотрудников больницы является важным моментом в деятельности всего учреждения.

# Аналитическая часть:

## Общая характеристика объекта защиты или исследования:

Частная урологическая клиника

## Обзор и анализ существующих систем

Система по составлению электронных медицинских карт и разработка веб приложения с защитой персональных данных не является новой в мире, подобные проблемы пытаются решить множество других приложений и программ. Но каждая команда разработчиков схожих приложений имеет свои правила, и инструкции по введению, выводу и хранении данных, что означает не каждая программа соответствует потребностям и предпочтениям потребителя. Для того чтобы охватить широкий круг пользователей в этой сфере разработчики пытаются создать многофункциональную программу или приложение. Что существенно облегчает работу операторов и админов, но тем самым с этой многофункциональностью приводит к утечки данных. Потому что количество объектов, подлежащих к защите увеличивается.

Так как учет персональных данных, справок, направлений и других медицинских документов является специфичной задачей программных обеспечений, специализированных для учета персональных данных данной категории лиц в открытых источниках, отсутствует.

К примеру, для рассмотрения схожего приложения возьмем «Electronic health record» который также специализируется в области работы с персональными данными в медицинской сфере. В приложении «Electronic health record» **сотрудники** или пациенты хранят всю основную персональную информацию, необходимую для проверки или сдачи анализов, использования в нужных ситуациях предоставления медицинской карты и простой осмотр в больнице.

* + 1. Таблица Сравнение существующих систем

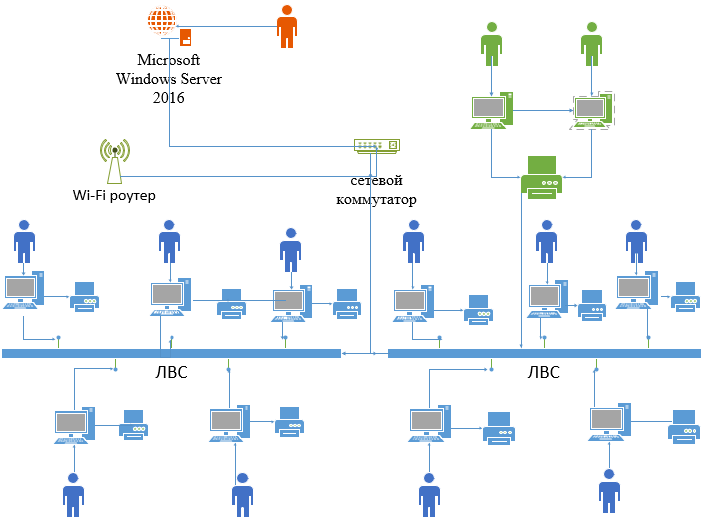
|  |  |  |  |
| --- | --- | --- | --- |
|  | **Electronic health record** | **Электронная Медицинская Карта РФ** | **Медицинская информационная система** |
| **Удобный и понятный интерфейс** | Есть | Есть | Есть |
| **Возможность экспортировать данные в файлы** | Есть такая возможность | Есть такая возможность | Есть такая возможность |
| **Работа в многопользовательск ом режиме** | Не предназначена | Есть такая возможность | Есть такая возможность |
| **Защита персональных данных** | Не предусмотрено | Не предусмотрено | Есть |
| **Защита БД** | Логин и пароль | Логин и пароль | Двухфакторная аутентификация |
| **Управления доступом пользователя к ЭМК** | Частично | Частично | Ролевая модель контроля за доступом |

Самый главный недостаток этих программ является избыточность функции. Нет возможности быстро проконсультироваться с врачом. Уточнить график работы или точный кабинет нужного сотрудника больницы. Узкое направление основной идеи приложения.

## Описание системы:

Объектом исследования данной работы является информационная система частного урологического центра, которая устроена следующим образом.

В нём работает 18 сотрудников, из них 10 врачей, 2 сотрудника приёмной и 6 работников персонала (охранники, санитары, медсестры). Всего в центре установлено 12 компьютеров, 11 принтеров и 1 сетевой коммутатор. У каждого врача и сотрудников приёмной есть свой персональный компьютер, на котором установлена операционная система Windows. В ней же и происходит основная часть их работы, принтеры модели Canon i-SENSYS MF3010. Все компьютеры объединены в локальную вычислительную сеть при помощи сетевого коммутатора серии XGS4600, фирмы Zyxell. Также в урологическом центре установлен Wi-Fi роутер компании TP-Link, версии TL-WR841 N300, обеспечивающий беспроводной доступ в интернет.



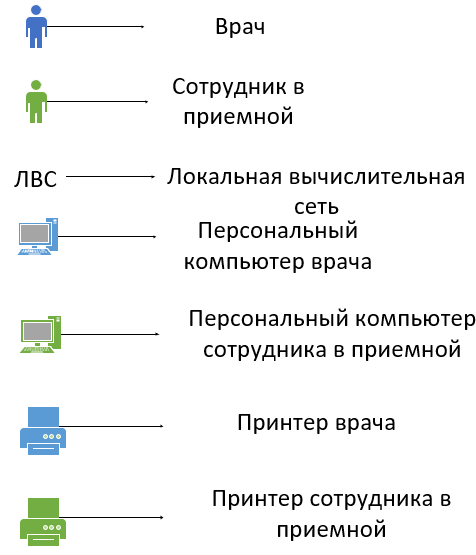


Рис.1.Схема, демонстрирующая оборудовании в системе

## Концептуальная модель

Для формулировки требований к функциональному поведению проектируемой системы разработана концептуальная модель разрабатываемой системы.

Концептуальная модель разрабатываемой системы изображена на рисунках и схем в виде UML–диаграммы вариантов использования (Use Case). Каждый вариант использования определяет последовательность действий, которые должны быть выполнены проектируемой системой при взаимодействии ее с соответствующим пользователем. Пользователь – это любой внешний фактор по отношению к моделируемой системе, который взаимодействует с системой и использует ее функциональные возможности для достижения определенных целей или решения частных задач.

В системе предусмотрены следующие типы пользователей разрабатываемой системы:

«Пользователи» - Пациенты, «Персонал медучреждения» - Врачи, медсестры и т.д.,

«Администратор» - Главврач, «Персонал Здравоохранения».

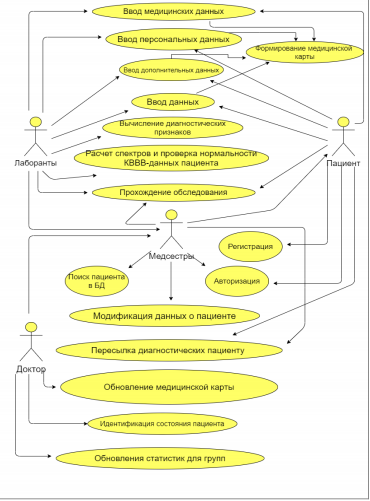


рис 4. Use-Case Продемонстрирована схема аутентификации

учетной записи пациента и заполнение нужных параметров.

Перед приёмом пациент проходит регистрацию в приёмной, он сообщает свою ФИО работнику приёмной. В приёмной работают два человека. У каждого из них есть свой персональный компьютер, на котором установлена операционная система Windows 10 почтовый клиент, текстовые редакторы, интернет-браузеры и другие приложения, необходимые для работы сотрудника. После чего сотрудник приёмной авторизуется в системе и ищет пациента по ФИО в базе данных. Если же пациент впервые проходит курс лечение в данном центре, ему необходимо открыть электронную медицинскую карту. Новую карту можно открыть в приёмной, для этого необходимо предоставить паспорт и пройти регистрацию у сотрудника приёмной. Карта содержит в себе ФИО пациента, его адрес, паспортные данные и историю болезней и посещений. После получения электронной карты, все данные о пациенте, его лечащие врачи, его диагнозы, анализы и история посещений будут записываться в неё. Сама электронная медицинская карточка хранится в базе данных, которая обрабатывается на сервере. Каждому пациенту необходимо пройти через регистрацию, после чего он может проходить курс лечения.

## Контекстная диаграмма AS-IS

При рассмотрение информационных потоков были выделены следующие пользователи:

* врач
* пациент
* системный администратор
* и используемые ими бизнес-приложения:
* клиентское приложение
* интернет-браузер

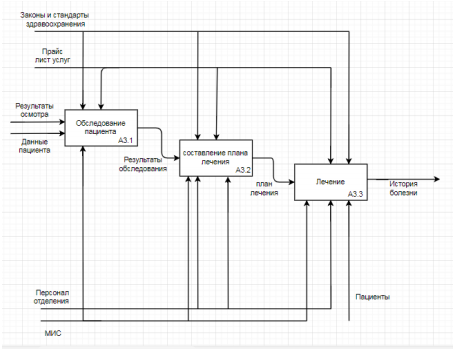
Схема основного процесса информационной системы урологической частной клиники (рис.2).



Рис.2.Схема главного процесса учреждения

## Контекстная диаграмма TO-BE

Схема, демонстрирующая информационные потоки, внутри частного урологического центра рис. 3.

рис.3.Схема взаимосвязи процессов в системе

## Основные процессы и информационные потоки:

Основным назначением информационной системы является создание электронной медицинской карты, введение в неё новых записей анализов и диагнозов, а также хранение её в базе данных.

В рамках выполнения данной работы были выделены следующие бизнес-процессы:

* Обработка информации - Урологический центр хранит данные о своих пациентах. Они находятся в базе данных, и посторонние люди не умеют доступа к ним.
* Приём анализов – это процесс взятия анализов пациента для постановки диагнозов выявления причин заболевания и дальнейшего оказания лечения.
* Ввод данных о пациенте в ЭМК – Врачи при осмотре вносят диагнозы, результаты анализов и прописывают курс лечения в ЭМК.
* Печать документа – Врачи распечатывают для пациентов рецепты, справки и направления.
* Обеспечение доступа к информации – этот процесс выполняется администратором. Он следит за тем, чтобы у врачей всегда был доступ к своим пациентам.
* Регистрация пациента – этот процесс осуществляется сотрудниками приёмной. Они создают новую ЭМК для новых пациентов, и заполняют её на основании паспорта.
* Формирование отчётов – этот процесс создания отчетов для ведения отчетности о проведённой работе.

В процессе своей работы врачи взаимодействуют с пациентами. Они записывают их диагнозы и прописывают курс лечения в электронную медицинскую карту. Сотрудники приёмной регистрируют новых пациентов урологического центра в базе данных пациентов.

## Модель потоков данных

С помощью модели потоков данных (DFD) было описано преобразование потоков данных в системе. Было создано диаграмма DFD модели TO-BE разрабатываемой системы. Эта модель описывает преобразование данных от входа до пользователя системы. На Рис.4. показано, что в систему поступают данные такие как: Конфиденциальные данные, Персональные данные, Информации об истории болезни и смс подтверждения от пользователей системы: Пользователи (Пациенты), Персонала Медучреждения. Администратор безопасности регулирует весь поток информаций, полученный от пользователей и персонала медучреждения тем самым, обновляет аудит базы данных, резервной копии и управляет доступом всей системы.



*Рис.4. Модель потоков данных*

Декомпозиция диаграммы (рис.5) потоков данных более подробно показывает работу системы

# Теоретическая часть

## Идентификация активов:

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»:

Актив - все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

Примечание. К активам организации могут относиться:

- активы информационные, в том числе различные виды информации, циркулирующие в системе информационной (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

- ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);

- процессы (технологические, информационные и пр.);

- выпускаемая продукция и/или оказываемые услуги [1].

Далее представлена таблица соответствия активов процессам частного урологического центра:

Таблица 1. Идентификация активов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Процесс ы*** | ***Информационны й актив*** | ***Приорите ты*** | ***Среда обработки ИА*** | ***Уязвимость безопасности*** |
|  |  |  | Windows 8-10 | Уязвимость компонента State Repository Service операционной системы Windows, позволяющая |
| ***Регистр ация пациент ов*** | Сведения о пациенте, персональные данные пациента | Конфиден циальност ь, Доступнос ть Целостнос ть | нарушителю повысить свои привилегии или выполнить произвольный код |
| Linux Ubuntu 16.04 | Уязвимость программного обеспечения Firefox, Firefox-esr, связанная с непринятием мер по защите структуры веб-страницы, позволяющая нарушителю оказать воздействие на целостность данных |
| Интернет Браузеры | Уязвимость сервера Microsoft Internet Information Server (IIS) операционных систем Windows, позволяющая нарушителю выполнить атаку типа «межсайтовая подделка запросов» |
|  |  |  | Windows 8-10 | Уязвимость компонента win32k операционной системы Windows, позволяющая нарушителю |
| ***Заполне ние история болезни пациент а*** | Сведение болезни пациента, история болезни пациента, медицинская книжка | Доступнос ть, Целостнос ть | раскрыть защищаемую информацию |
| Linux Ubuntu 16.04 | Уязвимость модуля отображения WebKit операционных систем iOS, tvOS, мультимедийного проигрывателя iTunes for Windows, браузера Safari и сервиса iCloud for Windows, позволяющая нарушителю раскрыть защищаемую информацию |
| Андроид и iOs платформах | Уязвимость механизма навигации в Android браузера Google Chrome, позволяющая нарушителю оказать воздействие на целостность данных |
| ***Регистр ация врачей*** | Персональные данные врача, его адресные, контактные данные, данные родственников, детали его квалификации | Конфиден циальност ь, Доступнос ть, Целостнос ть | Linux Ubuntu 16.04 | Уязвимость в коде, отвечающем за построение DNS-ответов DNS-сервера Dnsmasq, позволяющая нарушителю вызвать отказ в обслуживании или выполнить произвольный код |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Windows 8-10 | Уязвимость компонента Media Foundation операционных систем Windows, позволяющая нарушителю раскрыть защищаемую информацию |
| ***Редакти рование данных*** | История болезни, сведения о здоровье, рецепты, назначение на лечение | Доступнос ть, Целостнос ть, Конфиден циальност ь, | Windows 8-10 | Уязвимость компонента Windows Media Foundation операционных систем Windows, позволяющая нарушителю установить программы, просматривать, изменять или удалять данные с правами авторизованного пользователя |
| iOs платформа | Уязвимость операционных систем iOS, tvOS, macOS, watchOS, браузера Safari, мультимедийного проигрывателя iTunes для операционных систем Windows и сервиса iCloud для операционных систем Windows, вызванная целочисленным переполнением, позволяющая нарушителю выполнить произвольный код |
| PostgreSQL | Уязвимость реализации функций json\_populate\_recordset и jsonb\_populate\_recordset системы управления базами данных PostgreSQL, позволяющая нарушителю вызвать отказ в обслуживании или получить несанкционированный доступ к защищаемой информации |
| ***Обмен данным и*** | персональные данные, документы о состояние пациента, отчеты о пациентах, отчеты в МинЗдрав | Целостнос ть | Linux Ubuntu 16.04 | Уязвимость функции HandleRFBServerMessage кроссплатформенной библиотеки LibVNCServer, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании |
| PostgreSQL | Уязвимость скрипта pg\_ctlcluster из пакета postgresql-common система управления базами данных PostgreSQL, позволяющая нарушителю получить несанкционированный доступ к конфиденциальным данным, вызвать отказ в обслуживании и оказать воздействие на целостность данных |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Направление/пер енаправление между медучреждениям и*** | Рецепты на лечение, направление на анализы, | Целостнос ть | PostgreSQL | Уязвимость реализации команды «INSERT ... ON CONFLICT DO UPDATE» системы управления базами данных PostgreSQL, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации |
| Linux Ubuntu 16.04 | Уязвимость ядра операционных систем Linux, связанная со смещением указателя за пределы допустимых значений, позволяющая нарушителю реализовать атаки по побочным каналам |
| ***Назначение врача*** | Назначение врача на лечение, направление на ЛПУ | Конфиден циальност ь, Целостнос ть | Linux Ubuntu 16.04 | Уязвимость реализации класса PHP DirectoryIterator интерпретатора языка программирования PHP, позволяющая нарушителю раскрыть защищаемую информацию |
| PostgreSQL | Уязвимость библиотеки libpq системы управления базами данных PostgreSQL, позволяющая нарушителю реализовать атаку типа «человек посередине» |
| ***Обработка анализа пациента*** | Результаты анализа и обследование пациента, назначение на лечение | Конфиден циальност ь, Целостнос ть | Windows 8-10 | Уязвимость исполняемого файла NmAPI.exe системы мониторинга сетевой инфраструктуры WhatsUp Gold, позволяющая нарушителю получить несанкционированный доступ к системе WatsUp Gold или выполнить удаленные команды |
| Linux Ubuntu 16.04 | Уязвимость функции L2CAP\_PARSE\_CONF\_RSP ядра операционных систем Linux, позволяющая нарушителю получить доступ к защищаемой информации |
| Интернет Браузеры | Уязвимость обработчика сценариев VBScript браузера Internet Explorer, позволяющая нарушителю выполнить произвольный код |
| ***Выдача электронных справок и сведения о состояние*** | Справки, сведения о состояние пациента, сведения о лечение | Доступнос ть, Целостнос ть | Linux Ubuntu 16.04 | Уязвимость функции whereLoopAddBtreeIndex системы управления базами данных SQLite, позволяющая нарушителю вызвать отказ в обслуживании |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Интернет Браузеры | Уязвимость функции антивирусного сканирования средств антивирусной защиты Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Free, Kaspersky Security Cloud, Kaspersky Small Office Security для Windows, Kaspersky Endpoint Security для Windows, Kaspersky Internet Security для macOS, Kaspersky Endpoint Security для Linux, позволяющая нарушителю удалить произвольные файлы в системе |
| ***Отчетность больницы о сведение пациента и качество обслуживание врачей для Главврача*** | Сведение обслуживаю щих персоналов и пациентов, качество осмотра, пациентов отзывы о больнице | Конфиден циальност ь Доступнос ть Целостнос ть | Интернет Браузеры | Уязвимость антивирусных программных средств McAfee Total Protection (MTP), McAfee Anti-Virus Plus (AVP), McAfee Internet Security (MIS), связанная с недостатками загрузки сторонних файлов и проверки их цифровой подписи, позволяющая нарушителю повысить свои привилегии и выполнить вредоносный код |
| PostgreSQL | Уязвимость реализации функций json\_populate\_recordset и jsonb\_populate\_recordset системы управления базами данных PostgreSQL, позволяющая нарушителю вызвать отказ в обслуживании или получить несанкционированный доступ к защищаемой информации |
| ***Отчетность сведение о болезни и масштабности, лекарственные затраты, для МинЗдрава*** | Масштабност ь болезни по всей республики, Аналитика медучрежден ии, BIGDATA  анализы | Конфиден циальност ь Доступнос ть, Целостнос ть | Linux Ubuntu 16.04 | Уязвимость функции L2CAP\_GET\_CONF\_OPT ядра операционных систем Linux, позволяющая нарушителю получить доступ к защищаемой информации |
| Windows 8-10 | Уязвимость функции оптимизации производительности Lazy FPU context switching процессоров Intel Core, связанная с отсутствием защиты служебных данных, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации |

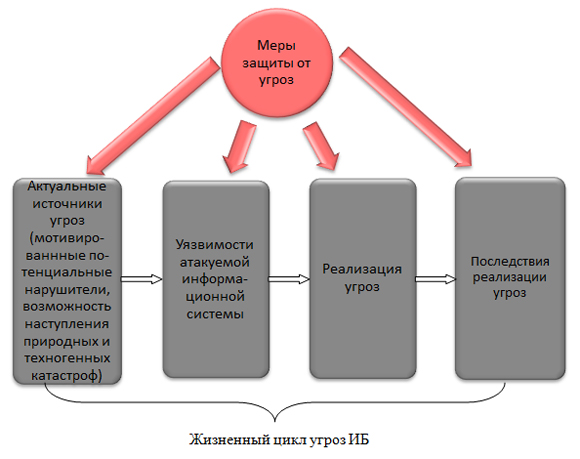
## Модели информационной безопасности:

### Модель угроз ИБ урологического центра:

**Угроза**  — это потенциальная возможность определенным образом нарушить свойства ИБ. Модель угроз информационной безопасности – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

Стандарт СТО БР ИББС – 1.0-2010 определяет модель угроз информационной безопасности следующим образом: это «описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба».

Адекватные модели угроз информационной безопасности позволяют выявить существующие угрозы, разработать эффективные контрмеры, повысив тем самым уровень ИБ, и оптимизировать затраты на защиту (сфокусировав её на актуальных угрозах).



В модели должны учитываться все актуальные угрозы на всех стадиях их жизненного цикла

У различных информационных систем, а также объектов одной информационной системы может быть разный спектр угроз, определяемый особенностями конкретной информационной системы и её объектов и характером возможных действий источника угрозы.

Процедура построения модели угроз информационной безопасности состоит из нескольких последовательных шагов:

* Определение источников угроз.
* Выявление критических объектов информационной системы.
* Определение перечня угроз для каждого критического объекта.
* Выявление способов реализации угроз.

Оценка материального ущерба и других последствий возможной реализации угроз. Основной целью злоумышленников является компрометация информационных активов персональных компьютеров. В такой ситуации можно выделить три типа актуальных угроз информационной безопасности:

* Нарушение целостности информации, обрабатываемой и внутри урологического центра. Примеры нарушений при обеспечении целостности:
* модификация (искажение) информации;
* навязывание ложной информации.
* Нарушение доступности информации, обрабатываемой и передаваемой внутри урологического центра. Примеры нарушений при обеспечении доступности:
* уничтожение информации и средств ее обработки.
* Нарушение конфиденциальности информации, представляющей собой личные данные каждого пациента. Примеры нарушений при обеспечении конфиденциальности:
* хищение (копирование) информации и средств ее обработки;
* утрата или разглашение (неумышленная потеря, утечка) информации и средств ее обработки.

Модели угроз составляются на основе постоянно меняющихся данных и поэтому должны регулярно пересматриваться и обновляться. Модель угроз ИБ ИС урологического центра приведена в Приложении А

## Модель нарушителя ИБ урологического центра:

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники. Все источники угроз безопасности информации можно разделить на три основные группы:

* Обусловленные действиями субъекта (антропогенные источники угроз).
* Обусловленные техническими средствами (техногенные источники угрозы).
* Обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.  
  
Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

криминальные структуры;

* потенциальные преступники и хакеры;
* недобросовестные партнеры;
* технический персонал поставщиков телематических услуг;
* представители надзорных организаций и аварийных служб;

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

* основной персонал (врачи, сотрудники приёмной);
* вспомогательный персонал (уборщики, охрана);
* технический персонал (системный администратор);

Самой большой угрозой урологического центра может быть халатность её сотрудников. Например, работники приёмной могут уйти со своего рабочего места без блокировки своего персонального компьютера, тем злоумышленник может воспользоваться компьютером сотрудника и завладеть информацией, к которой он должен был иметь доступ. Также на урологический центр может быть направлена DDoS-атака со стороны хакеров, которые захотели попробовать взломать базу данных и завладеть конфиденциальной информацией о пациентах данного учреждения. Данные хранящиеся в электронной медицинской карте должны оставаться известны только врачам, которые непосредственно лечили пациента, и никому более.

Техногенные источники угроз также могут оказать большой вред функционированию информационной системы частного урологического центра. Этот вид содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление. В центре не установлены резервные генераторы для бесперебойного обеспечения электроэнергией. Это может послужить большой проблемой для бесперебойного функционирования самого центра, а также его информационной системы. Также в центре отсутствует система предохранители на случаи резких скачков электроэнергии, что в последствии может привести к повреждению персональных компьютеров, потере несохраненных данных и т.д. Источником такого вида угрозы могут быть:

* сети инженерных коммуникации (водоснабжения, канализации);
* некачественные технические средства обработки информации;
* некачественные программные средства обработки информации;
* вспомогательные средства (охраны, сигнализации, телефонии);
* другие технические средства, применяемые в учреждении;
* Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе[17](https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml#17) в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.  
    
  Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:
* пожары;
* землетрясения;
* различные непредвиденные обстоятельства;
* другие форс-мажорные обстоятельства.

К нарушителям типа А относятся сотрудники организации, имеющие физический доступ ко всем персональным компьютерам. К ним можно отнести работников приёмной, которые в корыстных целях могут скомпрометировать личные данные пациентов, хранящуюся в урологическом центра.

Лица, относящиеся к нарушителям типа Б, являются компьютерными злоумышленниками, которые пытаются удаленно получить доступ к базе данных пациентов с целью получения личных данных.

Нарушителями типа В, являются люди, имеющие физический доступ на территорию урологического центра, однако не имеющие права работы с персональными компьютерами. К данному типу нарушителей могут относится стажеры, работники компаний оказывающие услуги по доставке воды, сотрудники службы поддержи интернет провайдера.

К нарушителям типа Г могут относиться сотрудники организации, имеющие право работы с информационной системой, а также имеющие к ней как физический, так и логический доступ. К ним относятся системные администраторы, имеющие право и возможность настраивать параметры передачи данных с помощью персональных компьютеров врачей, модифицировать параметры портов для считывания поступающей информации

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на: нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе. Потенциал нарушителей и их возможности приведены в таблице 7

Таблица 7.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Потенциал нарушителей | Виды нарушителей | Возможности по реализации угроз безопасности информации |
| 1 | Нарушители с базовым (низким) потенциалом | Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем, бывшие работники, лица, привлекаемые для установки различного оборудования. | Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему. |
| 2 | Нарушители с базовым повышенным (средним) потенциалом | Конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администратор информационной системы и администратор безопасности информационной системы. | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 3 | Нарушители с высоким потенциалом | Хакеры, уволенные сотрудники центра. | Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений |

## Политика ИБ урологического центра

Политика информационной [безопасности](https://arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html) – это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности. Политика информационной безопасности АИС урологического центра определяет цели и задачи обеспечения информационной безопасности при ее работе и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуются сотрудники в своей деятельности.

В ходе выполнения работы был разработан проект документа «Политика ИБ урологического центра». Политика ИБ сети разработана на основе анализа исходных данных объекта исследования, законодательства, нормативных и правовых документов органов исполнительной власти с учетом требований по безопасности, предъявляемым к информационным системам, а также в соответствии с Политикой информационной безопасности Организации, в частности на основании следующих документов:

1. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. От 19.12.2016) «Об информации, информационных технологиях и о защите информации» (с изм. И доп., вступ. В силу с 01.01.2017).
3. Модель угроз и модель нарушителя ИБ Урологического центра.

### Структура Политики ИБ урологического центра

Политика ИБ АИС Урологического центра является частной политикой информационной безопасности. В структуре документа можно выделить следующие ключевые разделы:

1. Введение – в данном разделе кратко описано назначение документа.
2. Цели и задачи обеспечения ИБ Урологического центра – данный раздел определяет цели и задачи Политики, которые будут достигнуты применением положений Политики.
3. Область действия – данный раздел определяет границы области действия требований Политики.
4. Описание активов ИБ Урологического центра – данный раздел определяет активы объекта защиты, по отношению к которым будут применяться требования Политики.
5. Описание угроз ИБ Урологического центра – данный раздел определяет актуальные угрозы ИБ для объекта защиты.
6. Требования и правила – данный раздел определяет требования по отношению к активам объекта защиты.
7. Субъекты политики ИБ Урологического центра – данный раздел определяет роли субъектов и их ответственность за обеспечение ИБ АИС Урологического центра в ходе работы с активами.
8. Повышение осведомленности в области ИБ – в данном разделе описан процесс повышения осведомленности сотрудников в области ИБ.
9. Контроль реализации – данный раздел описывает меры наказания за несоблюдение требований Политики, а также в нем определены ответственные лица за соблюдение и выполнение требований Политики.
10. Пересмотр политики ИБ АИС Урологического центра – в данном разделе определенна периодичность внесения изменений в Политику.

### Общие сведения о Политике ИБ АИС Урологического центра

Политика информационной безопасности устанавливает ответственность руководства, а также описывает подход организации к управлению информационной безопасностью АИС Урологического центра.

Требования Политики распространяются на всех сотрудников АИС Урологического центра. При любом замеченном инциденте ИБ, который может вызвать негативные последствия для функционирования АИС Урологического центра, связанные с нарушением ИБ, сотрудники должны незамедлительно сообщать об этом непосредственному руководителю и администратору.

Все случаи нарушения информационной безопасности подлежат индивидуальному расследованию.

### Субъекты Политики ИБ

К субъектам Политики ИБ АИС Урологического центра относятся следующие сотрудники:

1. Врачи
2. Сотрудники приёмной.
3. Системный администратор

### Пересмотр Политики ИБ

Положения Политики безопасности требуют регулярного пересмотра и корректировки не реже одного раза в год. Внеплановый пересмотр Политики безопасности проводится в случае:

* внесения существенных изменений в урологическом центре;
* возникновения инцидентов информационной безопасности.

При внесении изменений в положения Политики безопасности учитываются:

* результаты аудита информационной безопасности;

рекомендации независимых экспертов по информационной безопасности.

# Проектная часть

## Актуальность угроз ИБ:

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы. Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 4

Таблица 4.

|  |  |  |  |
| --- | --- | --- | --- |
| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
| Низкий | Средний | Высокий | |
| По наличию соединения с сетями общего пользования:  ИСПДн, имеющая многоточечный выход в сеть общего пользования;  ИСПДн, имеющая одноточечный выход в сеть общего пользования;  ИСПДн, физически отделенная от сети общего пользования | +  -  - | -  + | -  -  + | |
| По встроенным (легальным) операциям с записями баз персональных данных:  чтение, поиск;  запись, удаление, сортировка;  модификация, передача | +  +  + | -  -  - | -  -  - | |
| По разграничению доступа к персональным данным:  ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;  ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн  ИСПДн с открытым доступом | -  +  + | +  -  - | -  -  - | |
| По уровню обобщения (обезличивания) ПДн:  ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);  ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;  ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | -  -  + | -  +  - | +  -  - | |
| По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:  ИСПДн, предоставляющая всю базу данных с ПДн;  ИСПДн, предоставляющая часть ПДн; | +  - | -  + | -  - | |
| По территориальному размещению:  распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;  городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);  корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;  локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;  локальная ИСПДн, развернутая в пределах одного здания | +  +  -  -  - | -  -  +  +  - | -  -  -  -  + | |

Исходная степень защищенности определяется следующим образом:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2. При составлении перечня актуальных угроз безопасности ПДн каждой 9 степени исходной защищенности ставится в соответствие числовой коэффициент Y1, а именно:

* 0 – для высокой степени исходной защищенности;
* 5 – для средней степени исходной защищенности;
* 10 – для низкой степени исходной защищенности.

Согласно подсчетам:

1. ИСПДн не имеет высокий уровень исходной защищенности, так как лишь 21% характеристики ИСПДн равны высокому уровню.
2. ИСПДн не имеет средний уровень исходной защищенности, так как не выполняется условие по первому пункту и 32% характеристик равны среднему уровню.
3. ИСПДн имеет низкий уровень исходной защищенности, потому что не выполняются условия по пунктам 1 и 2.

Определены числовые коэффициенты исходной защищенности Y1 в соответствии угроз информационной безопасности в таблице 5.

Таблица 5

|  |  |  |
| --- | --- | --- |
| № | Угроза ИБ | Y1 |
| 1. | Угроза хищения информации (Windows 10  (ОС персонального компьютера)) | 10 |
| 2. | Угроза хищения информации (MsSQLServer) | 0 |
| 3. | Угроза нарушения доступности (Windows 10  (ОС персонального компьютера)) | 10 |
| 4. | Угроза нарушения доступности (MsSQLServer) | 0 |
| 5. | Угроза уничтожения информации (Windows 10  (ОС персонального компьютера)) | 5 |
| 6. | Угроза уничтожения информации (MsSQLServer) | 0 |
| 7. | Угроза изменения данных (Windows 10  (ОС персонального компьютера)) | 5 |
| 8. | Угроза изменения данных (MsSQLServer) | 0 |
| 9. | НСД к персональному компьютеру (Windows 10  (ОС персонального компьютера)) | 10 |
| 10. | НСД к персональному компьютеру (MsSQLServer) | 0 |
| 11. | Удаленное получение документов, отправленных на сетевой принтер | 10 |
| 12. | Перехват аутентификационных данных | 5 |
| 13. | Сбой в работе ОС (Источник-Антропогенный) | 5 |
| 14. | Сбой в работе ОС (Источник-Техногенный) | 0 |
| 15. | Сбои подачи электроэнергии (Windows 10  (ОС персонального компьютера)) | 5 |
| 16. | Сбои подачи электроэнергии (Microsoft Windows Server 2016) | 0 |

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

* маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
* низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
* средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
* высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

* 0 – для маловероятной угрозы;
* 2 – для низкой вероятности угрозы;
* 5 – для средней вероятности угрозы;
* 10 – для высокой вероятности угрозы.

Ниже показаны числовые коэффициенты Y2 вероятности возникновения угрозы каждой угрозы безопасности ПДн в таблице 6.

Таблица 6

|  |  |  |
| --- | --- | --- |
| № | Угроза ИБ | Y2 |
| 1. | Угроза хищения информации (Windows 10  (ОС персонального компьютера)) | 10 |
| 2. | Угроза хищения информации (MsSQLServer) | 2 |
| 3. | Угроза нарушения доступности (Windows 10  (ОС персонального компьютера)) | 5 |
| 4. | Угроза нарушения доступности (MsSQLServer) | 5 |
| 5. | Угроза уничтожения информации (Windows 10  (ОС персонального компьютера)) | 5 |
| 6. | Угроза уничтожения информации (MsSQLServer) | 2 |
| 7. | Угроза изменения данных (Windows 10  (ОС персонального компьютера)) | 5 |
| 8. | Угроза изменения данных (MsSQLServer) | 0 |
| 9. | НСД к персональному компьютеру (Windows 10  (ОС персонального компьютера)) | 10 |
| 10. | НСД к персональному компьютеру (MsSQLServer) | 0 |
| 11. | Удаленное получение документов, отправленных на сетевой принтер | 10 |
| 12. | Перехват аутентификационных данных | 5 |
| 13. | Сбой в работе ОС (Источник-Антропогенный) | 10 |
| 14. | Сбой в работе ОС (Источник-Техногенный) | 2 |
| 15. | Сбои подачи электроэнергии (Windows 10  (ОС персонального компьютера)) | 2 |
| 16. | Сбои подачи электроэнергии (Microsoft Windows Server 2016) | 0 |

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

Y = (Y1 +Y2)/ 20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

* если 0 ≤ Y ≤ 0,3 , то возможность реализации угрозы признается низкой;
* если 0,3 < Y ≤ 0,6 , то возможность реализации угрозы признается средней;
* если 0,6 < Y ≤ 0,8 , то возможность реализации угрозы признается высокой;
* если Y > 0,8 , то возможность реализации угрозы признается очень высокой.

По указанной формуле были вычислены коэффициенты и вербальная интерпретация реализуемости угрозы Y в таблице 7

Таблица 7

|  |  |  |  |
| --- | --- | --- | --- |
| № | Угроза ИБ | Y | Показатель реализуемости угрозы |
| 1. | Угроза хищения информации (Windows 10  (ОС персонального компьютера)) | 1 | Очень высокий |
| 2. | Угроза хищения информации (MsSQLServer) | 0,1 | Низкий |
| 3. | Угроза нарушения доступности (Windows 10  (ОС персонального компьютера)) | 0,75 | Высокий |
| 4. | Угроза нарушения доступности (MsSQLServer) | 0,25 | низкий |
| 5. | Угроза уничтожения информации (Windows 10  (ОС персонального компьютера)) | 0,5 | Средний |
| 6. | Угроза уничтожения информации (MsSQLServer) | 0,1 | Низкий |
| 7. | Угроза изменения данных (Windows 10  (ОС персонального компьютера)) | 0,5 | Средний |
| 8. | Угроза изменения данных (MsSQLServer) | 0 | Низкий |
| 9. | НСД к персональному компьютеру (Windows 10  (ОС персонального компьютера)) | 1 | Очень высокий |
| 10. | НСД к персональному компьютеру (MsSQLServer) | 0 | Низкий |
| 11. | Удаленное получение документов, отправленных на сетевой принтер | 1 | Очень высокий |
| 12. | Перехват аутентификационных данных | 0,5 | Средний |
| 13. | Сбой в работе ОС (Источник-Антропогенный) | 0,75 | Высокий |
| 14. | Сбой в работе ОС (Источник-Техногенный) | 0,1 | Низкий |
| 15. | Сбои подачи электроэнергии (Windows 10  (ОС персонального компьютера)) | 0,35 | Средний |
| 16. | Сбои подачи электроэнергии (Microsoft Windows Server 2016) | 0 | Низкий |

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения: низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных; 10

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

В результате оценки опасности каждой угрозы были определены показатели опасности ИСПДн в таблице 8.

Таблица 8

|  |  |  |
| --- | --- | --- |
| № | Угроза ИБ | Показатель опасности угрозы |
| 1. | Угроза хищения информации (Windows 10  (ОС персонального компьютера)) | Средняя опасность |
| 2. | Угроза хищения информации (MsSQLServer) | Высокая опасность |
| 3. | Угроза нарушения доступности (Windows 10  (ОС персонального компьютера)) | Низкая опасность |
| 4. | Угроза нарушения доступности (MsSQLServer) | Высокая опасность |
| 5. | Угроза уничтожения информации (Windows 10  (ОС персонального компьютера)) | Средняя опасность |
| 6. | Угроза уничтожения информации (MsSQLServer) | Высокая опасность |
| 7. | Угроза изменения данных (Windows 10  (ОС персонального компьютера)) | Средняя опасность |
| 8. | Угроза изменения данных (MsSQLServer) | Средняя опасность |
| 9. | НСД к персональному компьютеру (Windows 10  (ОС персонального компьютера)) | Средняя опасность |
| 10. | НСД к персональному компьютеру (MsSQLServer) | Высокая опасность |
| 11. | Удаленное получение документов, отправленных на сетевой принтер | Низкая опасность |
| 12. | Перехват аутентификационных данных | Высокая опасность |
| 13. | Сбой в работе ОС (Источник-Антропогенный) | Высокая опасность |
| 14. | Сбой в работе ОС (Источник-Техногенный) | Средняя опасность |
| 15. | Сбои подачи электроэнергии (Windows 10  (ОС персонального компьютера)) | Низкая опасность |
| 16. | Сбои подачи электроэнергии (Microsoft Windows Server 2016) | Высокая опасность |

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 9.

Таблица 9.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

По результатам расчетов, выявлены актуальные угрозы для данной ИСПДн из общего перечня угроз безопасности в таблице 10.

Таблица 10

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | – Угроза изменения данных (MsSQLServer)  – Сбой в работе ОС (Источник-Техногенный) | – Угроза хищения информации (MsSQLServer)  – Угроза нарушения доступности (MsSQLServer)  – Угроза уничтожения информации (MsSQLServer)  – НСД к персональному компьютеру (MsSQLServer)  – Сбои подачи электроэнергии (Microsoft Windows Server 2016) |
| Средняя | – Сбои подачи электроэнергии (Windows 10  (ОС персонального компьютера)) | – Угроза уничтожения информации (Windows 10  (ОС персонального компьютера))  – Угроза изменения данных (Windows 10  (ОС персонального компьютера)) | –Перехват аутентификационных данных |
| Высокая | – Угроза нарушения доступности (Windows 10  (ОС персонального компьютера)) |  | – Сбой в работе ОС (Источник-Антропогенный) |
| Очень высокая | – Удаленное получение документов, отправленных на сетевой принтер | – Угроза хищения информации (Windows 10  (ОС персонального компьютера))  – НСД к персональному компьютеру (Windows 10  (ОС персонального компьютера)) |  |

## 

## Политика безопасности ИБ ИС Урологического центра

### Введение

Назначением данной Политики информационной безопасности информационной системы урологического центра является определение целей, задач, правил, практических приемов и руководящих принципов обеспечения ИБ активов ИС урологического центра.

### Цели и задачи политики ИБ

Целями настоящей политики ИБ является:

* обеспечение устойчивого функционирования ИС урологического центра за счет предотвращения реализации угроз ИБ его активам;
* сохранение конфиденциальности важных информационных ресурсов;
* повышение осведомленности пользователей в области возможных угроз, нацеленных на активы.

Основными задачами политики ИБ являются:

* разработка требований по обеспечению ИБ;
* контроль выполнения установленных требований по обеспечению ИБ;

### Область действия

Данная политика распространяется на врачей, сотрудников приёмной, администратора, а также на лиц, имеющих физический доступ к активам.

Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, выполняющий функции администратора информационной системы.

Сотрудники урологического центра обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

### Описание активов, подлежащих защите

Основным назначением информационной системы является создание электронной медицинской карты, введение в неё новых записей анализов и диагнозов, а также хранение её в базе данных.

В рамках выполнения данной работы были выделены следующие бизнес-процессы:

* Обработка информации - Урологический центр хранит данные о своих пациентах. Они находятся в базе данных, и посторонние люди не умеют доступа к ним.
* Приём анализов – это процесс взятия анализов пациента для постановки диагнозов выявления причин заболевания и дальнейшего оказания лечения.
* Ввод данных о пациенте в ЭМК – Врачи при осмотре вносят диагнозы, результаты анализов и прописывают курс лечения в ЭМК.
* Печать документа – Врачи распечатывают для пациентов рецепты, справки и направления.
* Обеспечение доступа к информации – этот процесс выполняется администратором. Он следит за тем, чтобы у врачей всегда был доступ к своим пациентам.
* Регистрация пациента – этот процесс осуществляется сотрудниками приёмной. Они создают новую ЭМК для новых пациентов, и заполняют её на основании паспорта.
* Формирование отчётов – этот процесс создания отчетов для ведения отчетности о проведённой работе.

В процессе своей работы врачи взаимодействуют с пациентами. Они записывают их диагнозы и прописывают курс лечения в электронную медицинскую карту. Сотрудники приёмной регистрируют новых пациентов урологического центра в базе данных пациентов.

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»:

Актив - все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

Примечание. К активам организации могут относиться:

- активы информационные, в том числе различные виды информации, циркулирующие в системе информационной (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

- ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);

- процессы (технологические, информационные и пр.);

- выпускаемая продукция и/или оказываемые услуги [1].

Таблица соответствия активов процессам частного урологического центра приведена в Таблице 1:

### Угрозы ИБ

У различных информационных систем, а также объектов одной информационной системы может быть разный спектр угроз, определяемый особенностями конкретной информационной системы и её объектов и характером возможных действий источника угрозы.

Процедура построения модели угроз информационной безопасности состоит из нескольких последовательных шагов:

* Определение источников угроз.
* Выявление критических объектов информационной системы.
* Определение перечня угроз для каждого критического объекта.
* Выявление способов реализации угроз.

Оценка материального ущерба и других последствий возможной реализации угроз. Основной целью злоумышленников является компрометация информационных активов персональных компьютеров. В такой ситуации можно выделить три типа актуальных угроз информационной безопасности:

* Нарушение целостности информации, обрабатываемой и внутри урологического центра. Примеры нарушений при обеспечении целостности:
* модификация (искажение) информации;
* навязывание ложной информации.
* Нарушение доступности информации, обрабатываемой и передаваемой внутри урологического центра. Примеры нарушений при обеспечении доступности:
* уничтожение информации и средств ее обработки.
* Нарушение конфиденциальности информации, представляющей собой личные данные каждого пациента. Примеры нарушений при обеспечении конфиденциальности:
* хищение (копирование) информации и средств ее обработки;
* утрата или разглашение (неумышленная потеря, утечка) информации и средств ее обработки.

Модели угроз составляются на основе постоянно меняющихся данных и поэтому должны регулярно пересматриваться и обновляться. Модель нарушителей ИБ ИС урологического центра содержит следующие типы:

К нарушителям типа А относятся сотрудники организации, имеющие физический доступ ко всем персональным компьютерам. К ним можно отнести работников приёмной, которые в корыстных целях могут скомпрометировать личные данные пациентов, хранящуюся в урологическом центра.

Лица, относящиеся к нарушителям типа Б, являются компьютерными злоумышленниками, которые пытаются удаленно получить доступ к базе данных пациентов с целью получения личных данных.

Нарушителями типа В, являются люди, имеющие физический доступ на территорию урологического центра, однако не имеющие права работы с персональными компьютерами. К данному типу нарушителей могут относится стажеры, работники компаний оказывающие услуги по доставке воды, сотрудники службы поддержи интернет провайдера.

К нарушителям типа Г могут относиться сотрудники организации, имеющие право работы с информационной системой, а также имеющие к ней как физический, так и логический доступ. К ним относятся системные администраторы, имеющие право и возможность настраивать параметры передачи данных с помощью персональных компьютеров врачей, модифицировать параметры портов для считывания поступающей информации

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на: нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

### Требования и правила

Указанный перечень правил и требований является минимальным необходимым для предотвращения реализации угроз, описанных выше в разделе 2:

1. Обеспечить осуществление контроля доступа к ИС урологического центра.
2. Обеспечить осуществление контроля подключения внешних носителей информации.
3. Обеспечить обязательное присутствие механизмов авторизации при входе в учетную запись в ИС.
4. Настроить блокирование компьютера при прерывании или завершении работы с личным ПК
5. Использовать механизмы блокирования несанкционированного копирования информации ограниченного доступа или представляющую собой интеллектуальную собственность.
6. Запретить использования паролей по умолчанию для любых устройств.
7. Использовать механизмы защиты от DoS-атак.
8. Контролировать совместимость версий обновляемого программного обеспечения (далее – ПО).
9. Использовать антивирусные средства и своевременно обновлять антивирусные базы.
10. Использовать пароли, неподверженные перебору по словарю.

### Субъекты Политики ИБ

К субъектам Политики ИБ АИС Урологического центра относятся следующие сотрудники:

* Врачи
* Сотрудники приёмной.
* Системный администратор

### Повышение осведомленности в области ИБ

Руководство и весь персонал ИС урологического центра должны быть своевременно осведомлены о возможных угрозах и рисках ИБ, связанных с эксплуатацией и работе с ИС урологического центра. Должно вестись обучение всех сотрудников основным вопросам обеспечения ИБ. Также в начале каждого учебного года со студентами должен проводиться инструктаж по работе.

### Контроль реализации Политики ИБ

Ответственность за контроль исполнения и актуальность настоящей Политики, а также за общее руководство обеспечением информационной безопасности ИС урологического центра возлагается на системного администратора данного учреждения.

За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами ИБ ИС урологического центра.

### Пересмотр Политики ИБ

Положения Политики безопасности требуют регулярного пересмотра и корректировки не реже одного раза в год. Внеплановый пересмотр Политики безопасности проводится в случае:

* внесения существенных изменений в урологическом центре;
* возникновения инцидентов информационной безопасности.

При внесении изменений в положения Политики безопасности учитываются:

* результаты аудита информационной безопасности;

рекомендации независимых экспертов по информационной безопасности.

## Модель угроз ИБ ИС Урологического центра

Таблица 1 Модель угроз ИБ.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Угроза ИБ | Источник угрозы ИБ | Актив | | | | Метод реализации угрозы ИБ на среду обработки ИА | Последствия реализации угрозы ИБ |
| ИА | Значимые свойства ИБ в порядке приоритета | Среда обработки ИА | Уязвимость среды обработки ИА | Для ИА |
| Сбои подачи электроэнергии | Техногенный | База данных | Доступность  Целостность | Microsoft Windows Server 2016 | Отсутствие устройства бесперебойного питания | Подача напряжения, не соответствующего требованиям аппаратного обеспечения | Прекращение работы базы данных. |
| Сбои подачи электроэнергии | Техногенный | Несохраненные данные о пациенте | Доступность  Целостность | Windows 10  (ОС персонального компьютера | Отсутствие устройства бесперебойного питания | Подача напряжения, не соответствующего требованиям аппаратного обеспечения | Утеря несохраненных данных. |
| Сбой в работе ОС | Техногенный | Несохраненные данные о пациенте | Доступность  Целостность | Windows 10  (ОС персонального компьютера | Отсутствие защиты от перепада напряжения | Подача напряжения, не соответствующего требованиям аппаратного обеспечения | Нарушение целостности и/или доступности информации |
| Сбой в работе ОС | Антропогенный | Несохраненные данные о пациенте | Доступность  Целостность | Windows 10  (ОС персонального компьютера | Отсутствие защиты от перепада напряжения | Подача напряжения, не соответствующего требованиям аппаратного обеспечения | Нарушение целостности и/или доступности информации |
| Перехват аутентификационных данных | Антропогенный | Аутентификационные данные | Конфиденциальность | Интернет-шлюз | Неконтролируемость маршрутизации в сети интернет | Компрометация интернет-шлюза  (подбор идентификатора последовательности и номера порта-отправителя) | Компрометация аутентификационных данных |

Продолжение таблицы 1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Угроза хищений информации | Антропогенный | ЭМК пациента | Конфиденциальность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза хищений информации | Антропогенный | ЭМК пациента | Конфиденциальность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза нарушения доступности | Антропогенный | ЭМК пациента | Доступность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза нарушения доступности | Антропогенный | ЭМК пациента | Доступность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза уничтожения информации | Антропогенный | ЭМК пациента | Доступность  Целостность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности почтовых сообщений |
| Угроза уничтожения информации | Антропогенный | ЭМК пациента | Доступность  Целостность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Компрометация информации |
| Угроза уничтожения информации | Антропогенный | ЭМК пациента | Доступность  Целостность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Компрометация информации |
| Угроза изменения данных | Антропогенный | ЭМК пациента | Целостность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение целостности информации |
| Угроза изменения данных | Антропогенный | ЭМК пациента | Целостность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение целостности информации |

Продолжение таблицы 1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| НСД к персональному компьютеру | Антропогенный | ЭМК пациента | Конфиденциальность Целостность Доступность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение конфиденциальности, целостности и доступности информации. |
| НСД к персональному компьютеру | Антропогенный | ЭМК пациента | Конфиденциальность Целостность Доступность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение конфиденциальности, целостности и доступности информации. |
| Удаленное получение документов, отправленных на сетевой принтер | Антропогенный | информация ограниченного доступа | Конфиденциальность | Сетевой принтер  [Canon i-SENSYS MF3010](https://www.canon.ru/for_home/product_finder/multifunctionals/laser/i-sensys_mf3010/) | Уязвимости программного обеспечения принтера, (CVE-2019-12255, CVE-2019-12262 и CVE-2019-12264) | Подключение к сетевому принтеру удаленно и получение истории напечатанных документов | Компрометация данных, отправленных на печать. Нарушение конфиденциальности. |

В таблице приведены все виды потенциальных угроз информационной безопасности урологического центра и возможности их реализации. Рассмотрев всех угрозы, были выделены основные угрозы. Таблица 3.

Таблица 3. Модель основных угроз

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Угроза хищения информации | Антропогенный | ЭМК пациента | Конфиденциальность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза хищения информации | Антропогенный | ЭМК пациента | Конфиденциальность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности и конфиденциальности информации |
| Угроза нарушения доступности | Антропогенный | ЭМК пациента | Доступность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Отсутствие методов защиты от DDoS-атак | Нарушение доступности и конфиденциальности информации |
| Угроза нарушения доступности | Антропогенный | ЭМК пациента | Доступность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Отсутствие методов защиты от DDoS-атак | Нарушение доступности и конфиденциальности информации |
| Угроза уничтожения информации | Антропогенный | ЭМК пациента | Доступность  Целостность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение доступности почтовых сообщений |
| Угроза уничтожения информации | Антропогенный | ЭМК пациента | Доступность  Целостность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Компрометация информации |
| Угроза изменения данных | Антропогенный | ЭМК пациента | Целостность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | При изменении да |
| Угроза изменения данных | Антропогенный | ЭМК пациента | Целостность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Нарушение целостности информации |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| НСД к персональному компьютеру | Антропогенный | ЭМК пациента | Конфиденциальность Целостность Доступность | MsSQLServer | Использование слабых паролей или паролей по умолчанию. Включение ненужных функций Базы данных. Некорректная настройка СУБД. Отсутствие методов защиты от DDoS-атак | Заражение ОС троянской программой. Использование метода «фишинг». | Получив доступ к ПК врача открывается доступ к базе данных больницы, вследствие чего злоумышленник получается доступ к персональным данным пациентов |
| НСД к персональному компьютеру | Антропогенный | ЭМК пациента | Конфиденциальность Целостность Доступность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Получив доступ к ПК врача открывается доступ к базе данных больницы, вследствие чего злоумышленник получает доступ к персональным данным пациентов |
| Удаленное получение документов, отправленных на сетевой принтер | Антропогенный | информация ограниченного доступа | Конфиденциальность | Сетевой принтер  [Canon i-SENSYS MF3010](https://www.canon.ru/for_home/product_finder/multifunctionals/laser/i-sensys_mf3010/) | Уязвимости программного обеспечения принтера, (CVE-2019-12255, CVE-2019-12262 и CVE-2019-12264) | Подключение к сетевому принтеру удаленно и получение истории напечатанных документов | Компрометация данных, отправленных на печать. |
| Угроза хищения анализов | Антропогенный | информация ограниченного доступа | Конфиденциальность  Целостность Доступность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Злоумышленник получает доступ к персональным данным пациентов |
| Угроза изменения анализов | Антропогенный | информация ограниченного доступа | Целостность  Доступность  Конфиденцальность | Windows 10  (ОС персонального компьютера) | Отсутствие защиты от НСД. Отсутствие Антивирусного ПО | Заражение ОС троянской программой. Использование метода «фишинг». | Злоумышленник получает доступ к персональным данным пациентов |

## Модель нарушителей ИБ ИС Урологического центра

Таблица 1. Модель нарушителя ИБ.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вид нарушителя | Тип нарушителя | Опыт и знания | Доступные ресурсы для реализации угрозы ИБ | Мотивация | Метод реализации угроз ИБ |
| Антропогенный,  Тип А  (Сотрудник организации) | Внутренний | Опыт и знания зависят от занимаемой им роли в работе урологического центра.  Владеет сведениями о территориальном расположении компонентов сетевых компонентов и помещении, в котором находятся сами компоненты, о реализованных методов физической и организационной защиты объекта | Физический доступ в здание/помещение, в котором находятся компоненты | Любопытство или желание самореализации;  Выявление компрометирующей информации для дальнейшей ее продажи и получения финансовой выгоды;  Месть | Атака непосредственно на инфраструктуру сети |
| Осуществление несанкционированного логического доступа к ресурсам при физическом доступе |
| Умышленное внедрение вредоносных программ |
| Недопустимое изменение характеристик технических средств, в том числе, разрушение или уничтожение технических средств |
| Антропогенный,  Тип Б  (Компьютерный злоумышленник) | Внешний | Опыт: продвинутый пользователь ПК.  Владеет сведениями об уязвимостях компонентов сети, всех реализованных методах защиты, протекающих внутри технологических процессов, методах и средствах реализации компьютерных атак | Логический доступ к сети,  Физический доступ к сетевому оборудованию | Любопытство или желание самореализации;  Выявление компрометирующей информации для дальнейшей ее продажи и получения финансовой выгоды;  Месть | Атака непосредственно на инфраструктуру сети |
| Осуществление несанкционированного логического доступа к ресурсам при физическом доступе |
| Умышленное внедрение вредоносных программ |
| Использование утраченных/похищенных носителей информации |
| Недопустимое изменение характеристик технических средств, в том числе, разрушение или уничтожение технических средств |
| Антропогенный Тип Г  Системные администраторы | Внутренний | Опыт: продвинутый пользователь ПК.  Владеет сведениями об инфраструктуре сети | Имеет физический доступ к оборудованию для работы сети, логический доступ сети.  физический доступ в здание/помещение, в котором находятся главные компоненты | Желание самореализации;  Выявление компрометирующей информации для дальнейшей ее продажи и получения финансовой выгоды;  Месть | Неисполнение или ненадлежащее исполнение своих должностных обязанностей, |
| Несоблюдение требований внутренних документов, регламентирующих деятельность по ИБ |
| Умышленное внедрение вредоносных программ |
| Умышленное использование активов в целях, отличных от целей функционирования сети по причине отсутствия персонала |