МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Разработка и внедрение политики информационной безопасности организации или учреждения»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

# **1 Обоснование актуальности**

В связи с интеграцией информационных технологий во все сферы, теперь без эффективной системы информационной безопасности, гарантировать конфиденциальность и сохранность данных невозможно. Поликлиникам, как и другим учреждениям, требуется защищать свои информационные ресурсы. Наличие персонализированных данных, часть из которых является врачебной тайной, вынуждает учреждения такого типа иметь передовые и новейшие технологии в области защиты информации.

Для оптимального решения этой задачи необходимо разработать политику информационной безопасности поликлиники, которой неукоснительно должны следовать все его служащие.

Цели политики информационной безопасности:

* Аунтефикация;
* Авторизация;
* Конфиденциальность;
* Целостность;
* Доступность;
* Защита ресурсов;
* Аудит безопасности;

Задачи разработки политики информационной безопасности:

* Установка объектов защиты;
* Установка основных угроз и их источников;
* Оценка угроз, рисков и уязвимостей;
* Установка мер, методов и средств обеспечения требуемого уровня защищенности информационных ресурсов;

## **Объекты защиты**

Основными объектами системы информационной безопасности в поликлиниках являются:

Эти данные могут стать объектом противоправного покушения, их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением, предусмотренным статьей 349 Уголовного кодекса РБ.

## **2.1 Структура поликлиники**

Информационная среда поликлиники является распределенной структурой, объединяющей участников в единую систему.

Структура поликлиники выглядит следующим образом:



* Старший инспектор по кадрам
* Главный бухгалтер
  + Бухгалтерия
* Главный врач
  + Начальник хозяйственной службы
  + Заместитель главного врача по медицинской части
  + Специалист по мобилизационной подготовке
  + Инженер по охране труда
  + Главная медицинская сестра

К основным особенностям информационной среды поликлиники относятся:

* широкая территориальная распределенность компонентов информационной системы;
* значительное расширение сферы использования автоматизированных систем обработки информации;
* абстрагирование владельцев данных от физических структур и места размещения данных (информации);
* наличие большого числа персонализированных данных;

## **2.2 Обзор объектов и субъектов информационных отношений**

Основные объекты защиты:

* Защищенные каналы передачи информации;
* Персонализированная информация клиентов;
* Программное обеспечение;
* Диски хранящие данные;

Основные субъекты защиты:

* Сотрудники поликлиники;
* Компьютеры сотрудников;

## **3 Основные угрозы и их источники**

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба предприятию в целом.

Перечень угроз безопасности включает атаки как внешнего, так и внутреннего происхождения. Информационные базы данных, принадлежащие поликлиник, могут стать объектами покушений хакеров.

Частыми целями преступных посягательств являются клиентские базы данных, содержащие информацию о номерах телефонов, местах проживания и медицинских историй посещения.

Кроме того, не исключен риск заражения компьютерных систем компании различными вирусами, которые могут причинить существенный ущерб в виде:

* блокировки доступа к важным файлам;
* уничтожения файлов;
* передачи информации третьим лицам.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на предприятие объективных физических процессов или стихийных природных явлений, независящих от человека. Среди естественных угроз можно

выделить:

* Сбои подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* Чрезвычайные ситуации (пожар, сбои работы электропитания, наводнения)

Искусственные угрозы – это угрозы предприятию, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные)
  + неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п., некомпетентное использование;
  + передача данных по незащищенным канал связи
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).
  + действия сотрудников поликлиники, направленные на получение персонализированной информации для последующего разглашения третьим лицам;
  + деятельность преступных групп, а также отдельных лиц по добыванию и/или искажению информации, нарушению работоспособности системы в целом или ее отдельных компонентов;
  + запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

## **4 Оценка угроз, рисков и уязвимостей**

|  |  |  |  |
| --- | --- | --- | --- |
| Атака | Ущерб | Вероятность | Риск |
| Кражи, нападения, взлом, саботаж и проникновение | 4 | 0,1 | 0,4 |
| Отказы и неисправности технических средств | 1 | 0,2 | 0,2 |
| Mailbombing | 2 | 0,3 | 0,6 |
| Отказ в обслуживании (Denial of Service - DoS) | 4 | 0,2 | 0,6 |
| Атака типа man-in-the-middle. | 3 | 0,3 | 0,9 |
| Фишинг | 3 | 0,3 | 0,9 |
| Копирование информации с жесткого диска, хранящего персональную информацию | 4 | 0,1 | 0,4 |
| Атака с анализаторами протоколов | 3 | 0,2 | 0,6 |
| Удаленное проникновение | 3 | 0,2 | 0,9 |
| Порча оборудования | 4 | 0,2 | 0,8 |
| Пожар | 4 | 0,1 | 0,4 |
| Наводнение | 4 | 0,1 | 0,4 |
| Передача данных по незащищённым каналам связи | 2 | 0,3 | 0,6 |
| Запуск сторонних технологических программ | 2 | 0,2 | 0,4 |
| Итого |  |  | 8,1 |

## **5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Все меры обеспечения безопасности информационной системы подразделяются на:

* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с персоналом информационной системы.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

К технологическим мерам защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений и т.п.

Организационные (административные) меры защиты — это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

### **5.1 Формирование политики безопасности**

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации поликлиники целесообразно разбить на два уровня. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

* каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;
* кто имеет права доступа к информации ограниченного распространения, кто и при каких условиях может читать и модифицировать информацию и т.д.;

### **5.2 Регламентация допуска сотрудников к использованию информационных ресурсов**

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационной системой поликлиники и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно, регламента предоставления доступа пользователей.

Основными пользователями информации в информационной системе являются сотрудники компании. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

* каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с сотрудниками, ответственным за информационное сопровождение данного ресурса;
* главный врач имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;
* наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и коммерческой тайны, а также правил работы с информацией.

Обработка информации в компонентах информационной системы должна производиться в соответствии с утвержденными технологическими инструкциями.

### **5.3 Подбор и подготовка персонала**

Пользователи информационной системы должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

### **5.4 Основные меры и требования обеспечения информационной безопасности**

Основные меры обеспечения информационной безопасности заключаются в следующем:

* формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы;
* подготовка решений по обеспечению конфиденциальности, доступности, целостности данных;
* наблюдение за функционированием системы защиты;
* разработка мер нейтрализации моделей возможных атак;
* обучение персонала правилам безопасной обработки информации;
* контроль за действиями персонала;
* принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;
* сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

Основные требования для обеспечения информационной безопасности в поликлинике:

* Наличие охраны, системы видеонаблюдения, сигнализаций на кабинетах с важными ресурсами системы или наличие пропускной системы с удостоверение личности рабочего персонала;
* Наличие отдела, отвечающего за ремонт технических средств;
* Наличие отдела, отвечающего за технологическое обеспечение;
* Разработка ПО предоставляющий безопасный канал связи;
* Закупка новейшего оборудования и мониторинг актуальности оборудования;
* Использования шифрования данных;
* Систематическое проведение бесед с персоналом о возможные последствиях при несоблюдении правил безопасности при работе со сторонними ресурсами;
* Введение аудита действия персонала;

### **Вывод**

Для учреждения поликлиника была разработана политика информационной безопасности, а также план мероприятий по её реализации. Были выделены основные субъекты и объекты, возможные угрозы и их источники. Была составлена оценка по возможным угрозам, где выделили: вероятность угрозы, возможный ущерб и риск. А на основе угроз были составлены меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.