Муниципальное автономное общеобразовательное учреждение средняя общеобразовательная школа №30 города Тюмени

имени Федора Ефимовича Федорова

**ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ**

по теме: «Информационная безопасность»

Выполнил: ученик 7 «В» класса,

Седельников Федор Александрович

Проверил: учитель математики,

Швецов Виталий Борисович

Тюмень – 2024

СОДЕРЖАНИЕ

|  |  |
| --- | --- |
| ВВЕДЕНИЕ | 3 |
| ГЛАВА 1. ТЕОРИТИЧЕСКИЕ АСПЕКТЫ ПОНЯТИЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ | 4 |
| 2. РАЗРАБОТКА МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАОУ СОШ №30 | 5 |
| ЗАКЛЮЧЕНИЕ | 8 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ | 10 |

ВВЕДЕНИЕ

На сегодняшний день 92% компаний, по данным «Gartner», не в состоянии обнаружить взломы на ранних стадиях, а именно таргетированные атаки, которые отличаются высокой скрытностью. [3]

Источниками угрозы являются как внешние злоумышленники, так и внутренние, а сама атака может быть направлена на любую информационную систему компании.

Поэтому тема выбранного проекта актуальна и практически значима.

Целью исследовательского проектаявляется выявление проблем и разработка мероприятий по информационной безопасности МАОУ СОШ №30.

Для реализации поставленной цели необходимо решить следующие задачи:

1. Дать понятие информационной безопасности.
2. Выявить узкие места в информационной безопасности МАОУ СОШ №30.
3. Разработать мероприятия по защите информационных данных и рассчитать их эффективность.

Объектом исследовательского проекта является МАОУ СОШ №30, предметом – информационная безопасность образовательной организации.

Гипотеза исследования: в рамках работы было рассмотрено предположение, что реализация мероприятия по информационной безопасности МАОУ СОШ №30, будет способствовать защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

В соответствии с поставленными целями, структурно исследовательский проект состоит из введения, 2 глав заключения и списка использованных источников и литературы.

ГЛАВА 1. ТЕОРИТИЧЕСКИЕ АСПЕКТЫ ПОНЯТИЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность– это совокупность методов, программно-технических и технологических средств, обеспечивающих сбор, накопление, обработку, хранение, представление и распространение информации.[1]

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Безопасность информации - состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и целостность. [1]

Поэтому система безопасности должна в первую очередь гарантировать доступность и целостность информации, а затем уже (если необходимо) ее конфиденциальность.

Принцип современной защиты информации можно выразить так - поиск оптимального соотношения между доступностью и безопасностью. [1]

На мой взгляд, информационная безопасность это не только коммуникация с внешней средой, а зашита своих данных от посягательств со стороны внутренней среды.

2. РАЗРАБОТКА МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАОУ СОШ №30

Проблемы информационной безопасности в МАОУ СОШ №30:

* Использование wi-fi школы для игр на переменах с сайтов носящих потенциальные угрозы.
* Не защищенность сети wi-fi школы.
* Редко обновляются пароли от сети wi-fi.
* Угроза информационной безопасности не извне, а изнутри образовательной организации.

Мероприятия по защите информационных данных представлены на рисунке 2.1.



Рисунок 2.1. - Мероприятия по защите информационных данных МАОУ СОШ №30

Согласно рисунку 2.1, мероприятия по защите информационных данных МАОУ СОШ №30 включают:

1. Мероприятия по защите wi-fi соединения: еженедельная смена паролей, обновление прошивки роутера, установка фильтра на МААс адреса, изменение имени используемой сети и настройку гостевой сети для компьютерного класса.

2. Внедрение программы «Цифровой купол».

Возможности программы «Цифровой купол»:

1. Управление сессиями пользователей во всех системах (поддерживающих OpenID Connect, OAuth).
2. Управление доступом пользователей к объектам доступа (Ролевая модель).
3. Генерация и выдача идентификационной информации
4. Управление идентификаторами.
5. Многофакторная аутентификация пользователей с использованием (Email, SMS, Push, TOTP).
6. Регистрация событий безопасности.
7. Обеспечение целостности.
8. Отслеживание фактов и факторов идентификации и аутентификации пользователей.

Преимущества программы «Цифровой купол» представлены на рисунке 2.2.

Согласно рисунку 2.2, к преимуществам программы «Цифровой купол» можно отнести:

- Централизованное решение на базе защищенной ИТ инфраструктуры

- Ролевая модель. Передача функции безопасности по ролевой модели в сертифицированное решение ПО.

- Закрытие требований по информационной безопасности в части несекционного доступа.

- Оптимизация вычислительных ресурсов замена secret net на АРМ пользователе.

- Сертификация МИБ в ФСТЭК России по 6 УД в 2023 году.



Рисунок 2.2 - Преимущества программы «Цифровой купол».[2]

Математическая модель процесса передачи данных через wi-fi соединение.

– хi – это процесс защиты wi-fi соединение на сервере;

– воздействия внешней среды на модель vi€, l=1, vi,

 где vi – это процесс передачи баз данных на сервере;

– внутренние параметры модели: hi€H, k=1,nk,

где nk – это процесс передачи баз данных через wi-fi соединение;

– выходные характеристики модели yj€Y, J=1,ny,

где yi – это объем загруженной информации.

Закон протекания процесса передачи данных через wi-fi соединение может быть представлен в общем виде:

y(t) =Qs(z,v,h,y), (1.1)

где Qs – оператор воздействия на модель.

ЗАКЛЮЧЕНИЕ

Цель проекта достигнута, задачи можно считать решенными.

Информационная безопасность – это информационная безопасность это не только коммуникация с внешней средой, а зашита данных от посягательств с внутренней стороны.

Среди проблем информационной безопасности МАОУ СОШ №30 можно выделить одну самую яркую - использование wi-fi школы для игр на переменах с сайтов, носящих потенциальные угрозы.

Среди основных проблем информационной безопасности в МАОУ СОШ №30 можно выделить одну самую яркую – использование паролей от компьютерного класса учениками в личных целях.

На основании выявленных проблем были разработаны мероприятия, направленные на защиту информационных данных.

Просчитаны затраты и их эффективность. Срок окупаемости предлагаемых мероприятий равен 1 год и 2 месяца.

В рамках исследовательского проекта построена математическая модель функционирования wi-fi соединения в МАОУ СОШ №30, которая может быть использована для имитационного моделирования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Информационная безопасность [Электронный ресурс]: https://lureit.ru/?yclid=5198923861788721151 (дата обращения 19.04.2024)

2. Цифровой купол. Типовой программный модуль информационной безопасности [Электронный ресурс]: https://digdes.ru/products/tsifrovoj-kupol (дата обращения 19.04.2024)

3. «Gartner» journal [Электронный ресурс]: https://www.gartner.com/en(дата обращения 19.04.2024)