Государственное бюджетное общеобразовательное учреждение города Оренбург «Школа № ??»

Индивидуальный проект на тему: «Защита данных»

ПРОЕКТ ДЕЛАЛА УЧЕНИЦА 9-ОГО КЛАССА «?» АННА (ФАМИЛИЯ)

РУКОВОДИТЕЛЬ ПРОЕКТА – (ПРЕПОД)

ОРЕНБУРГ 2023

Содержание.

Цель, актуальность, задача.

Цель исследования: понять и изучить для чего нужна защита данных, а также узнать, где они применяются.

Актуальность: недостаточно технологий для защиты данных, любая информация, имеющая финансовую или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры.

Задача: сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба организация.

Вводная часть.

Защитные данные имеют достаточно много способов и действий, ориентированных на защиту от несанкционированных действий с данными. Информация является сведениями, которые передаются в устной и письменной форме с помощью знаков, технических механизмов, жестов, программ. Информация и составляющие ее принципы до сих пор изучаются экспертами для повышения эффективности хранения и использования данных.

Она включает в себя:

1. данные, которые передаются между людьми и специализированными аппаратами;
2. знаки (у животных, растений);
3. другие отличительные свойства (клетки, органы).

Нужно понимать, что защита данных, применяется в различных средах таких как: политической, экономической, социальной и духовной.

Основная часть.

На первом этапе развития концепций обеспечения безопасности данных преимущество отдавалось программным средствам защиты. Когда практика показала, что для обеспечения безопасности данных этого недостаточно, интенсивное развитие получили всевозможные устройства и системы. Постепенно, по мере формирования системного подхода к проблеме обеспечения безопасности данных, возникла необходимость комплексного применения методов защиты и созданных на их основе средств и механизмов защиты. Обычно на предприятиях в зависимости от объема хранимых, передаваемых и обрабатываемых конфиденциальных данных за информационную безопасность отвечают отдельные специалисты или целые отделы.

Управление представляет собой регулирование использования всех ресурсов системы в рамках установленного технологического цикла обработки и передачи данных, где в качестве ресурсов рассматриваются технические средства.

Препятствия физически преграждают нарушителю путь к защищаемым данным.

Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

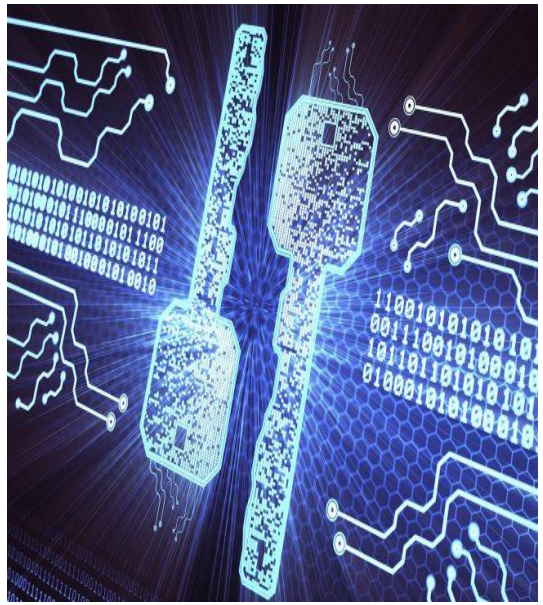
Регламентация как метод защиты заключается в разработке и реализации в процессе функционирования информационной системы комплексов мероприятий, создающих такие условия технологического цикла обработки данных.

Побуждение состоит в создании такой обстановки и условий, при которых правила обращения с защищенными данными регулируются моральными и нравственными нормами.

Принуждение включает угрозу материальной, административной и уголовной ответственности за нарушение правил обращения с защищенными данными.

Криптографические преобразования.

Про криптографические преобразования нужно поговорить отдельно. Есть два вида: шифрование и кодирование. Шифрование возможно осуществить с помощью нескольких методов. Шифрование заменой символов шифруемого текста заменяются другими символами (А-м, Б-л и т. д.); Шифрование методом перестановки шифрование с использованием ключей: если для шифрования и расшифровывания используется один ключ, то такой криптографический процесс называется симметричным. Недостаток этого процесса в том, что для передачи ключа надо использовать связь, а она должна тоже быть защищенной. Т. е. проблема повторяется. Поэтому в Интернет используют несимметричные криптографические системы, основанные на использовании не одного, а двух ключей, один открытый, а другой закрытый. Например, фирма отправляет клиенту квитанцию о том, что заказ принят к исполнению, она закодирует ее своим закрытым ключом, а клиент прочитает ее, воспользовавшись имеющимся у него публичным ключом данной фирмы.



Кодирование бывает двух типов: Смысловое по специальным таблицам и Символьное – по кодовым алфавитам.

Таким образом:

Показателями безопасности информации являются время, в течение которого обеспечивается определенный уровень безопасности.

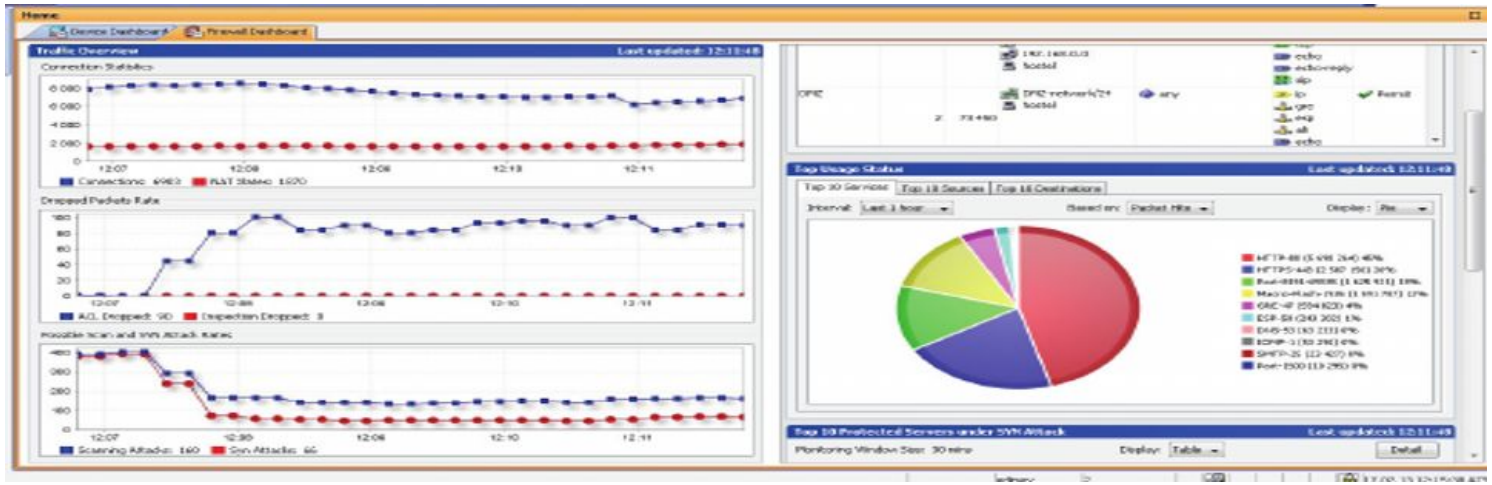
Основные виды защищаемой информации по содержанию: секретная и несекретная.

Собственный эксперимент.

План исследований: используем программное обеспечение для того, чтобы выявить входящего трафика в сеть, выбрать наиболее оптимальную технологию защиты информации.

Используя программное обеспечение, произведем структуру защитного экрана с целью понижения возможности прохождения атак.

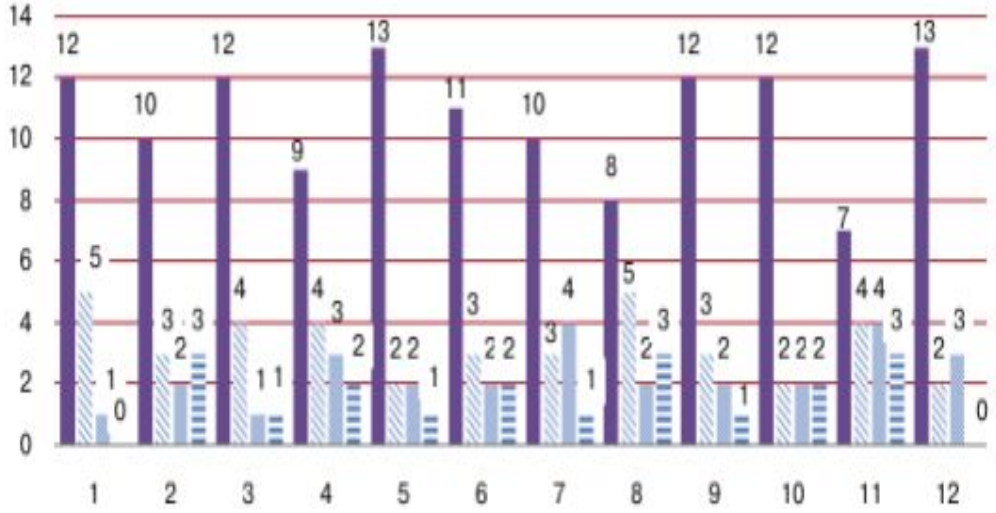
В ходе эксперимента на графикам мы можем наблюдать, как повышается эффективность загрузки канала после оптимизации.

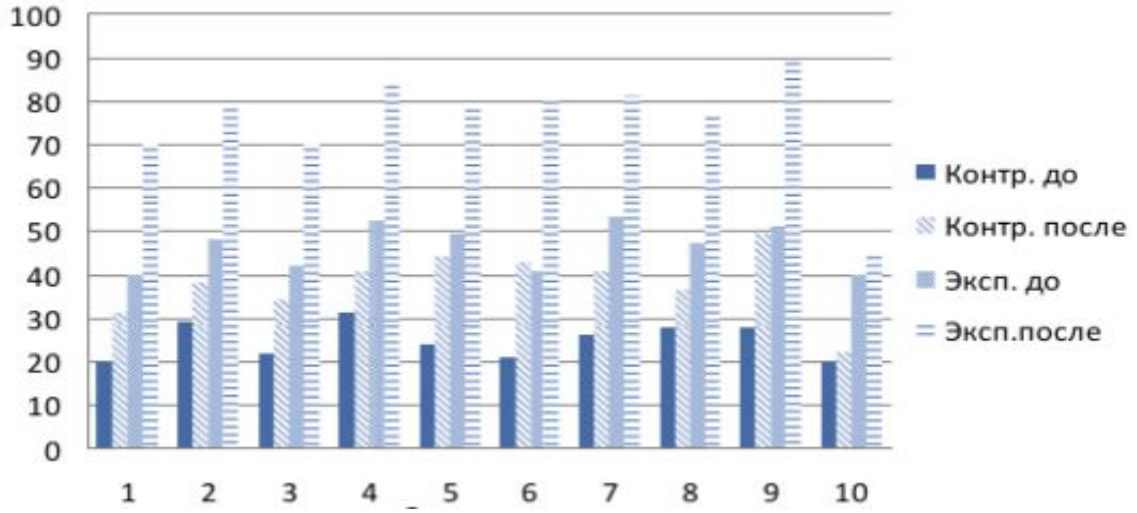


Заключение.

С помощью программного обеспечения можно выявить полноту усвоения, а также структуру унифицированной концепции защиты информации, стратегию защиты, и выявить возможное риски и угрозы для сети различных предприятий. Из всего этого можно сказать, что с помощью программное обеспечение можно минимизировать риски атаки сети.

Графики защиты информационных сетей.





Вывод моего проекта.

Подводя итог, можно с уверенностью сказать, что есть много различных программных обеспечений, с помощью которых можно улучшать защиту различных сетей для каких-либо предприятий. Защита данных предоставляет для пользователей полную безопасность, а также не допускает утечку конфиденциальной информации. Эти технологии очень нужны в нынешнее время, и это все должно развиваться дальше для более улучшенной защиты данных.

Источник информации.

- **Литература:**

Гафнер В.В. Информационная безопасность: Учеб. Пособие. – Ростов-на-Дону: Феникс, 2010

Григорьев С.Г. Методика проведения педагогического эксперимента. – М.; МГРПУ 2005.

Малюк А.А. Теория защиты информации. – М.; Горячая линия-Телеком, 2012.

Интернет ресурс:

https://cyberleninka.ru/article/n/eksperimentalnaya-proverka-effektivnosti-obucheniya-studentov-vuzov-tehnologiyam-zaschity-informatsii-v-usloviyah/viewer

https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/tseli-i-zadachi-informatsionnoj-bezopasnosti/

http://www.spsl.nsc.ru/naukresursy-i-uslugi-gpntb-so-ran-dlya-nauki-i-biznesae-i-biznesu/rdm/security/