



Муниципальное образовательное
учреждение
средняя общеобразовательная школа №
15

Исследовательский
проект
**Защита
информации**

Автор: Поляков Артемий Александрович,
учащийся 10-А класса
Руководитель: Бурькина Ольга Алексеевна,
учитель физики и информатики

Мичуринск
2022



Содержание

- **Введение.....3**
- История возникновения защиты информации.....4
- Средства защиты информации.....5
- Биометрический метод защиты.....9
- Виды киберпреступлений.....10



Задачи проекта:

- Узнать историю возникновения защиты информации.
- Выяснить современные методы и средства защиты информации.
- Выделить наиболее распространенные киберпреступления.
- Провести анкетирование среди людей по защите информации.

Цель проекта: узнать историю возникновения и развития информации, выяснить наиболее современные и распространенные виды киберпреступлений, а также средства и методы от них Провести анкетирование.



Введение



В настоящее время каждый человек обладает огромным количеством информации. Это неотъемлемая часть нашей жизни, мы постоянно что-то узнаем от окружающего нас мира. Чаще всего информацию хранят на электронных носителях. Само собой, возникает потребность в возникновении защиты информации от незаконного доступа. Но многие даже не задумываются и не осознают, что их информация может быть украдена или уничтожена, и оставляют её без всякой защиты. Если произойдет кража налоговой и банковской информации, то у человека могут возникнуть очень серьёзные проблемы. Особую осторожность нужно уделять при работе в сети, ведь тогда хакеру будет намного легче взломать ваши личные данные.

История возникновения

защиты информации

В. Н. Лопатин предполагает, что в истории человеческой цивилизации появление категории «информационная безопасность» связано с возникновением средств информационных коммуникаций и осознанием человеком возможности нанесения ущерба собственным интересам или интересам социальной системы посредством информационного обмена. Возникновение защиты информации делят на несколько этапов:

1
Этап

Он связан с естественным желанием человека и общества защитить информацию, которая обладает каким-либо уникальным значением

2
Этап

Использование информационно-коммуникационных технологий в процессе обеспечения информационной безопасности начинается.

3
Этап

Он связан с применением радиолокационных и гидроакустических средств.

4
Этап

Решение задач информационной защиты достигается с помощью электронно-вычислительных машин(ЭВМ).

5
Этап

Развитие технических средств информационной безопасности связан с созданием локальных информационных сетей.

6
Этап

Применение сверхмобильных коммуникационных механизмов, решающих высокотехнологичные задачи.

7
Этап

Характеризуется развитием глобальных информационных сетей и космических разработок.



Средства защиты информации

Нетехнические средства защиты информации:

- ▶ **Правовые средства защиты информации** - это метод, основанный на закреплении в законодательстве тех прав и законов, которые устанавливают меры защиты информации и препятствуют хакеру в совершении преступления, в случае пренебрежения законом назначается наказание различной меры тяжести.
- ▶ **Организационные средства защиты информации** - это внутренние правила, устанавливаемые компанией для блокирования доступа к информации постороннего круга людей.
- ▶ **Контроль доступа** - это метод, который заключается в определении подлинности субъекта и фиксации факта доступа.

Технические средства защиты информации:

- ▶ **Физические средства защиты информации** - это разнообразие устройств, которые воспрепятствуют и контролируют несанкционированный доступ к информации и её кражу.
- ▶ **Программные средства защиты информации** - это система специальных программ, которые включены в ПО, защищающие информацию от несанкционированного доступа.
- ▶ **Аппаратные средства защиты информации** - это средства, которые защищают информацию физическими методами и встроены в саму систему.
- ▶ **Криптографические средства защиты** - это такое преобразование информации, после которого она становится недоступной для обычного просмотра и использования лицами, не имеющими на это прав.





Биометрические системы защиты информации

Статические методы защиты

Динамические методы защиты

Биометрические системы защиты информации – это способ защиты информации, заключающийся в использовании биометрических данных людей для удостоверения личности. Бывают статические и динамические системы защиты.



Статические методы

- ✓ Дактилоскопия - способ, когда для распознавания личности используются отпечатки уникального рисунка линий на подушке пальца руки.
- ✓ Сканирование радужной оболочки глаза – сканирование радужной оболочки глаза для удостоверения личности.
- ✓ Распознавание по геометрии рук – это измерение определённых параметров человеческой кисти.
- ✓ Считывание геометрии лица - это автоматическая локализация человеческого лица на изображении или видео и, при необходимости, идентификация личности человека на основе имеющихся баз данных.

Динамические методы

- ✓ Распознавание голоса – это автоматический процесс преобразование речевого сигнала в цифровую информацию.
- ✓ Графологическое распознавание – это способ удостоверения личности с помощью считывания уникального графического почерка человека



Виды киберпреступлений

Киберпреступление – это преступная деятельность, целью которой является незаконная деятельность в виртуальном пространстве с использованием Интернета или какой-либо иной компьютерной сети



1

DoS-атака – это хакерская атака на вычислительную систему, с целью выведения её из строя

2

Ботнеты – это компьютерная сеть, в которой каждое устройство с доступом в интернет заражено вредоносной программой и управляется бот-мастером.

3

Кража онлайн-личности – это незаконная кража персональных данных пользователя, используемые в последствии для получения выгоды.

4

Киберсталкинг – это использование Интернета с целью домогательств и/или преследования человека, группы людей или целой организации. .

5

Социальная инженерия – это психологическая манипуляция над людьми, позволяющая хакеру получить конфиденциальную информацию жертвы.

6

Фишинг – это вид интернет-преступления, целью которого является завладение учетной записью пользователя или получение доступа к его компьютеру.

7

Онлайн-мошенничество – это вид мошенничества с использованием Интернета. .

