

Проект по информационной безопасности

Выполнили:

Орас Никита

Крупий Юлия

Садогурская Анастасия

Руководитель проекта:

Рылеева Алена Андреевна

Введение

Актуальность:

Множество важной и личной информации содержит наш компьютер. Возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий.

Цель проекта:

Рассмотреть способы защиты информации в современном мире.

Введение

Задачи:

Предотвращение угроз безопасности вследствие несанкционированных действий по уничтожению, искажению, копированию, блокированию информации или иных форм незаконного вмешательства в информационные ресурсы и информационных системах.

Понятие информационной безопасности

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.



Основные составляющие
информационной
безопасности

```
graph TD; A[Основные составляющие информационной безопасности] --> B[Доступность]; A --> C[Целостность]; A --> D[Конфиденциальность];
```

Доступность

Целостность

Конфиденциальность

Критерии классификации угроз

Угроза — возможность разрешения противоречия во взаимодействии объекта безопасности с другими объектами или во взаимодействии компонентов объекта безопасности между собой путём насильственного изменения в сторону ухудшения свойств одного из них, либо объекта безопасности в целом, т. е. путём нанесения вреда

Основание классификации

По месту
нахождения
источника
угроз

По типу
источника
угроз

По
вероятности
реализации
угроз

По ущербу
объекту
безопасности

По объекту
безопасности

Принцип работы антивирусных программ

Реактивная защита - защита от известных угроз с использованием знаний об участках кода и других уникальных особенностях существующих вредоносных программ. Для того чтобы такая защита работала успешно, антивирусная программа должна иметь обновленные базы сигнатур.

Проактивная защита - защита от новых вредоносных программ, основанная на знании неуникальных особенностей кода и поведения, характерных для деструктивного ПО.

АНТИВИРУСЫ

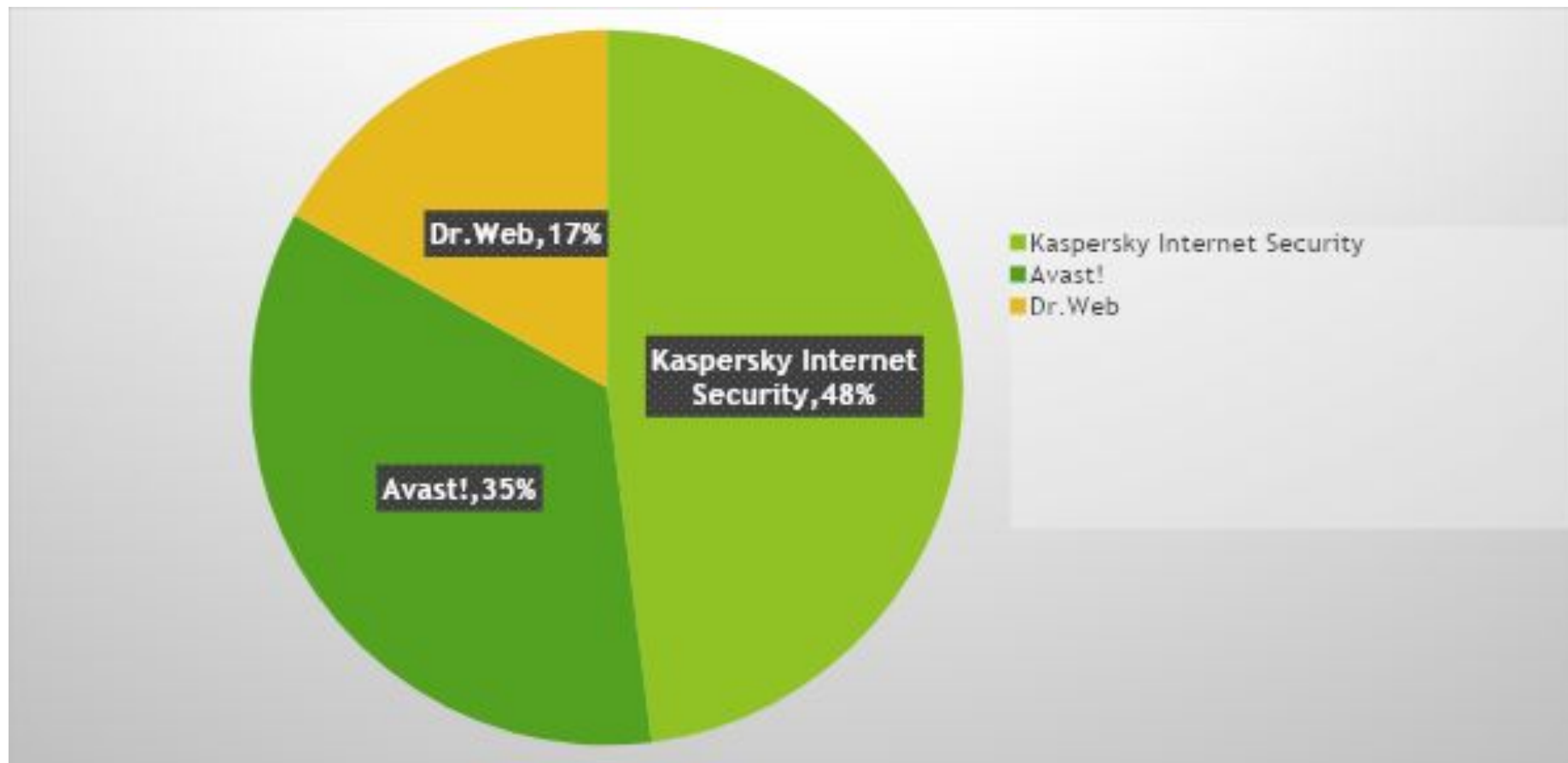


1. Kaspersky Antivirus обеспечивает защиту среднего класса, поскольку не контролирует сетевой трафик в полном объеме.

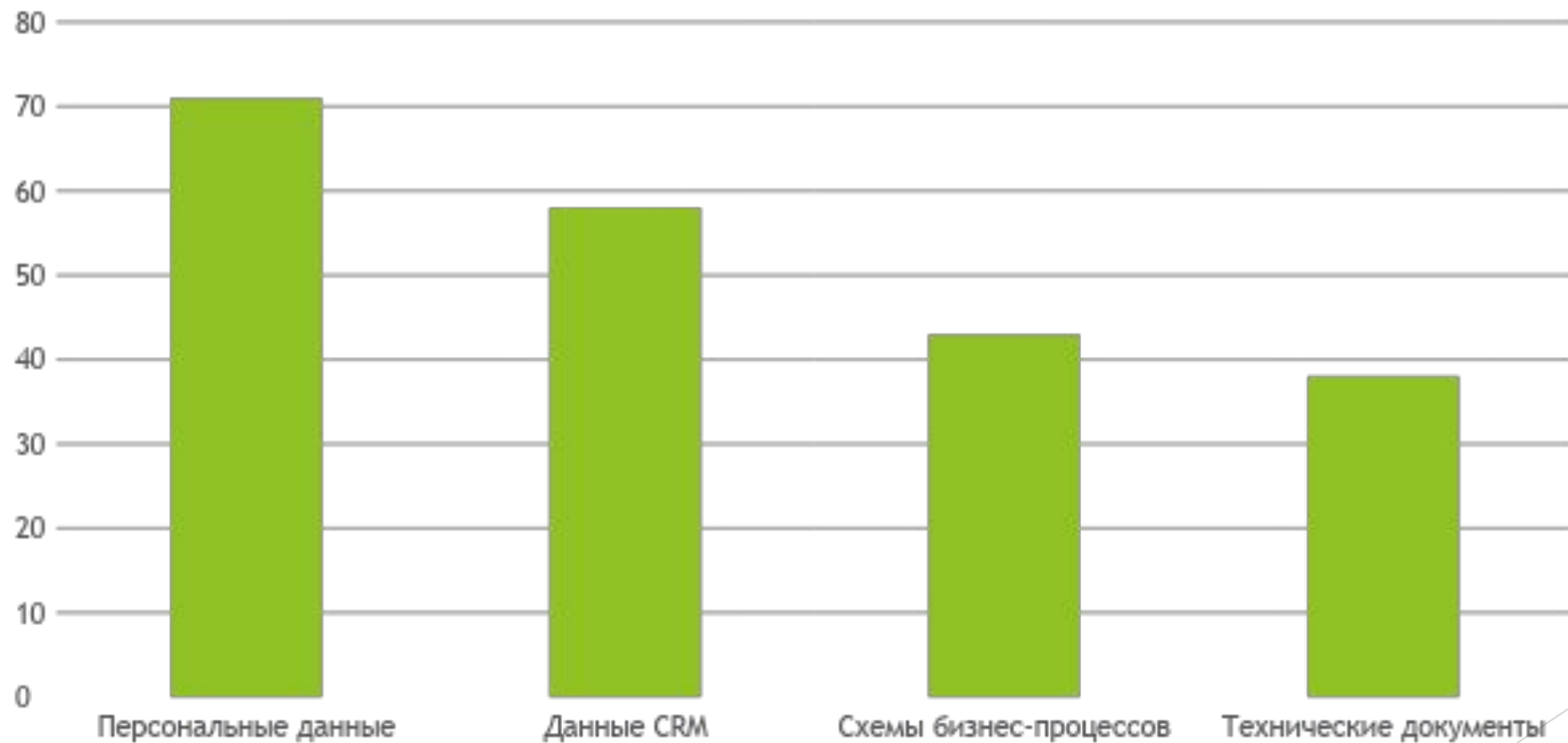
2. Avast! Антивирусная система, которая способна обнаруживать и ликвидировать различные виды вредоносных элементов.

3. Dr. WEB. Антивирусный вендор в мире, владеющий собственными уникальными технологиями детектирования.

Опрос: «Каким антивирусом вы пользуетесь?»»



Опрос: «Какая информация защищается в первую очередь?»



Методы взлома

1. Фишинг

Самый простой способ взлома - спросить у пользователя его/ее пароль. Фишинговое сообщение приводит ничего не подозревающего читателя на поддельные сайты онлайн-банкинга, платежных систем или иные сайты, на которых нужно обязательно ввести личные данные, чтобы "исправить какую-то страшную проблему с безопасностью".



Методы взлома

2. Социальная инженерия

Социальная инженерия придерживается той же концепции, что и фишинг - "спросить у пользователя пароль", но не с помощью почтового ящика, а в реальном мире. Любимый трюк социальной инженерии - позвонить в офис под видом сотрудника ИТ-безопасности и просто попросить пароль доступа к сети.



Методы взлома

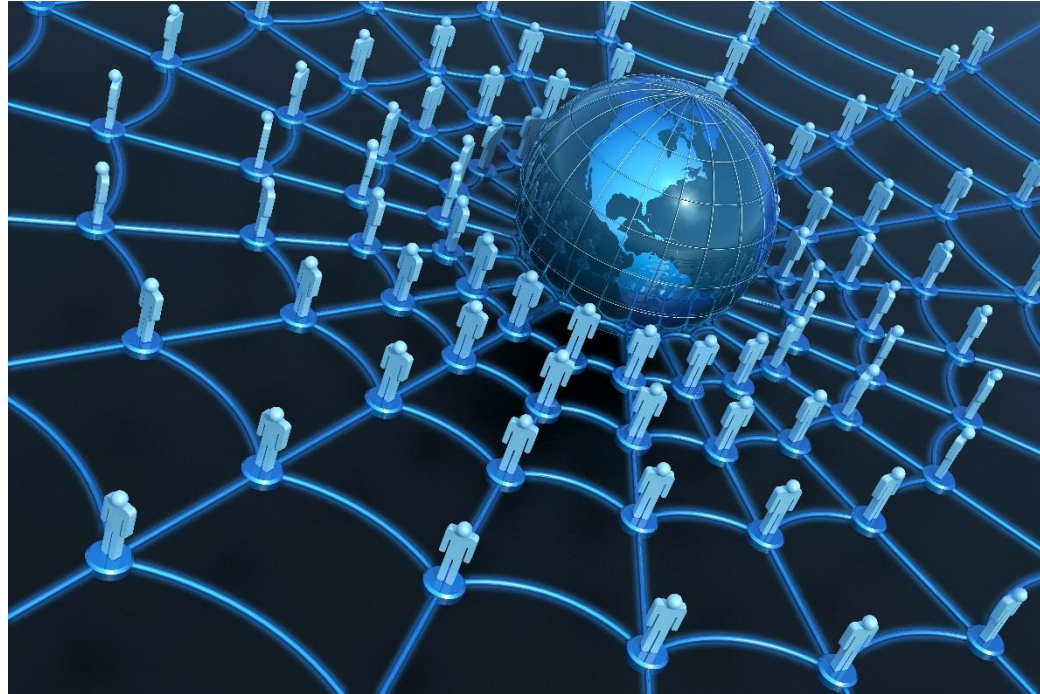
3. Вредоносное программное обеспечение

Программа перехвата вводимой с клавиатуры или выводимой на экран информации может быть установлена вредоносным ПО, которое фиксирует всю информацию, которую вы вводите, или создает скриншоты во время процесса авторизации, а затем направляет копию этого файла хакерам.

Методы взлома

4. Метод «пауков»

Опытные хакеры поняли, что многие корпоративные пароли состоят из слов, которые связаны с бизнесом. Действительно опытные хакеры автоматизировали процесс и запускают "паутинные" приложения, аналогичные тем, которые применяются ведущими поисковыми системами.



Способы защиты информации

```
graph TD; A[Способы защиты информации] --> B[Использование паролей]; A --> C[Шифрование]; A --> D[Электронная подпись];
```

Использование
паролей

Шифрование

Электронная
подпись

Заключение

В ходе исследования было выяснено, что защита информации - есть комплекс мероприятий, проводимых собственником информации. Понятие информационной безопасности - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий.