

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИМРСКИЙ КОЛЛЕДЖ»

Предметно-цикловая комиссия общеобразовательных
дисциплин Специальность/профессия

27.02.07 Управление качество продукции, процессов и услуг
(по отраслям)

Индивидуальный проект на тему: "Безопасность работы в сети интернет"

Обучающаяся: Крюкова София

Алексеевна Руководитель проекта:

Т.А. Соловьева

Год

2022

ВВЕДЕН

ИБ

- **Актуальность темы** обусловлена ростом большого числа пользователей без первоначальных навыков и умений в сфере компьютерных программ, не знающие ничего о правилах безопасности в сети, такие пользователь абсолютно безоружны перед возможными угрозами.
- **Цель проекта** заключается в изучении различных вредоносных программ и способов защиты от них, выявление методов по борьбе с вирусами, и выявление основных правил безопасности в интернете, основные способы заражения компьютера вредоносными программами.
- **Задачи проекта:** Изучить различные виды угроз безопасности в интернете; проанализировать методы защиты персональных данных в интернете; выявить основные способы заражения компьютера вредоносными программами.
- **Объектом исследования** являются ведущие IT-компании.
- **Предмет проекта** и формула различные IT-компании; изучить то, как функционируют различные вредоносные программы в интернете;
- **Период проекта:** с марта 2022 по июнь 2022

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

- **Вредоносные программы** – это термин, используемый для описания вредоносных приложений и кода, которые могут привести к повреждению и нарушению нормальной работы различных гаджетов. Вредоносные программы могут разрешить доступ посторонним, использовать ваши системные ресурсы, красть пароли, заблокировать вас на компьютере и попросить выкуп.
- Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.
- В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на следующие типы: компьютерный вирус, червь, троян, вирусы-блокировщики, боты
- **Червь** – это разновидность вредоносного программного обеспечения, которое копирует само себя с одного устройства на другое.
- **Троянская программа**— это вредоносный агент, основное отличие которого от классического вируса состоит в методе распространения: обычно он проникает в систему под видом обычной, легитимной программы, чем и обусловлена традиция называть его «троянским конем»
- **Вирусы блокировщики** — это вид вирусов, которые блокируют вашу операционную

СПОСОБЫ ЗАРАЗИТЬСЯ

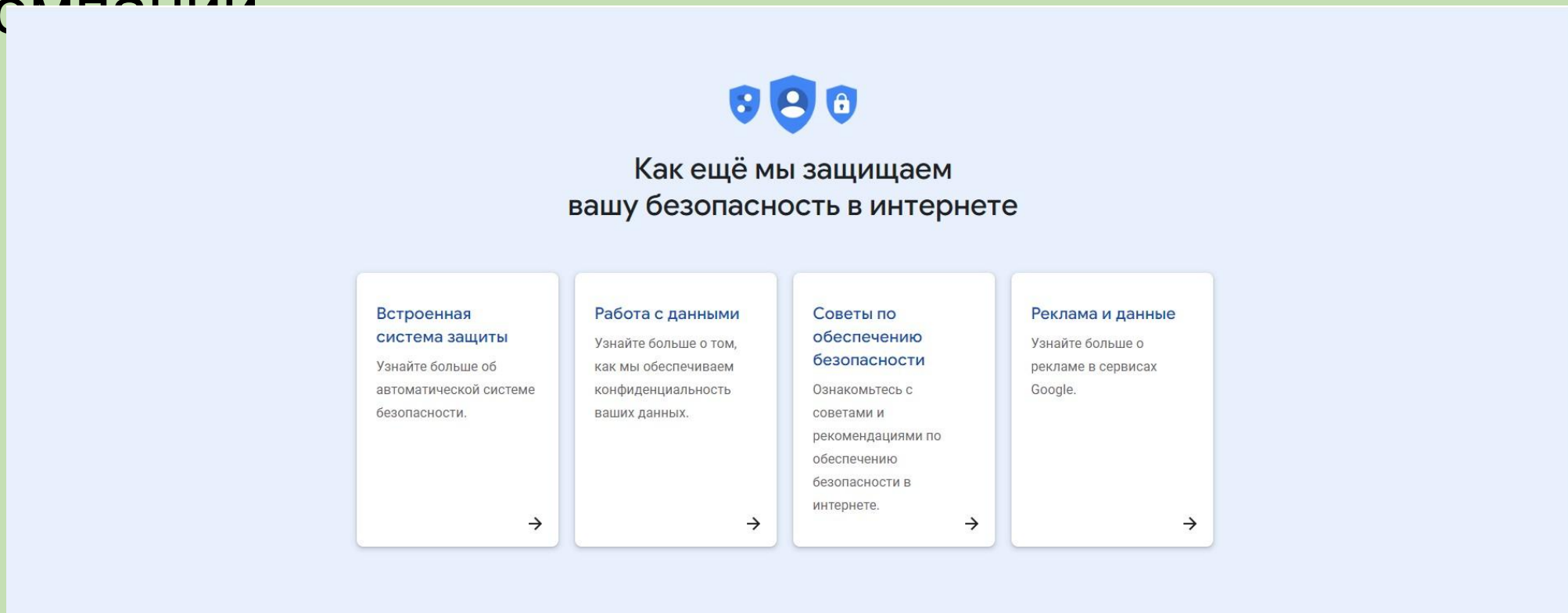
- Способов заражения ПК вирусами в интернете множество, рассмотрим основные из них: через флешки, через электронную почту, через интернет и локальные сети, через веб-страницы
- **Заражение вирусом через электронную почту** происходит следующим образом, вирус в самом письме или во вложениях в нём. Вам приходит письмо от неизвестного отправителя, вы открываете его, переходите по ссылке в нём или скачиваете и открываете вложения, в которых спрятался вирус.
- **Заражение вирусом через флешку** происходит при подключении переносного диска, планшета или смартфона через USB, например, для зарядки, существует ненулевая вероятность, что устройство будет заражено вредоносным ПО
- **Заражение через веб-страницы** происходит при открытии страницы, найденной в поисковике или через сообщение, клике по баннеру или по ссылке на другом сайте
- **Для защиты от вирусов можно использовать:** общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей; профилактические меры, позволяющие уменьшить

МЕТОДЫ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

- Для того, чтобы работа в сети Интернет была безопасна нужно соблюдать следующие правила:

1. никому не передавать конфиденциальные данные (логин, пароль), в том числе родственникам, коллегам;
2. исключать использование паролей по умолчанию, (второй год подряд самым популярным паролем в мире является «123456»);
3. регулярно запускать работу операционной системы и программного обеспечения с установленными обновлениями безопасности;
4. на всех устройствах, должно быть установлено лицензионное антивирусное программное обеспечение с актуальными обновлениями;
5. не использовать общественные беспроводные сети и устройства для работы с личной информацией не использовать программные продукты, полученные из сомнительных источников (пиринговые и файлообменные сети), модифицированные программные продукты,
6. не посещать ресурсы с сомнительной репутацией; личную информацию вводить только при безопасном соединении (URL веб-сайт должен начинаться с «https://», в интерфейсе браузера должна появиться иконка замка);
7. выполнять резервное копирование важной информации.

Рекомендации безопасной работы от ведущих IT-компаний



- Компания GOOGLE имеет встроенные системы защиты, и предлагает двухэтапную систему аутентификации
- Компания GOOGLE для обеспечения безопасности использует шифрование передаваемых данных. Когда вы отправляете письмо, открываете доступ к видео или посещаете сайт, происходит обмен информацией между вашим устройством, сервисами Google и центрами обработки данных.

ЗАКЛЮЧЕН ИЕ

- Интернет — это до сих пор очень опасное место, в котором очень много вирусов, и большинству людей приходится интуитивно справляться с этим, и пытаться сохранить свою безопасность.
- Основные выводы:
 1. Работа в сети Интернет — рискованное дело, в котором из-за одной маленькой ошибки, можно подхватить серьёзный вирус.
 2. Росту преступности в интернете способствует огромный ряд факторов, самый главный из которых — слишком большой объём информации, которую даже различные компании не успевают фильтровать.
 3. Основная причина того, что человек подхватил вирус в Интернете — переход по ссылке на подозрительном сайте или переход по ссылке из сообщения на почте.
 4. Качественный антивирус лучше всего обеспечит безопасность в интернете

и с ним можно избежать множества проблем, связанных с