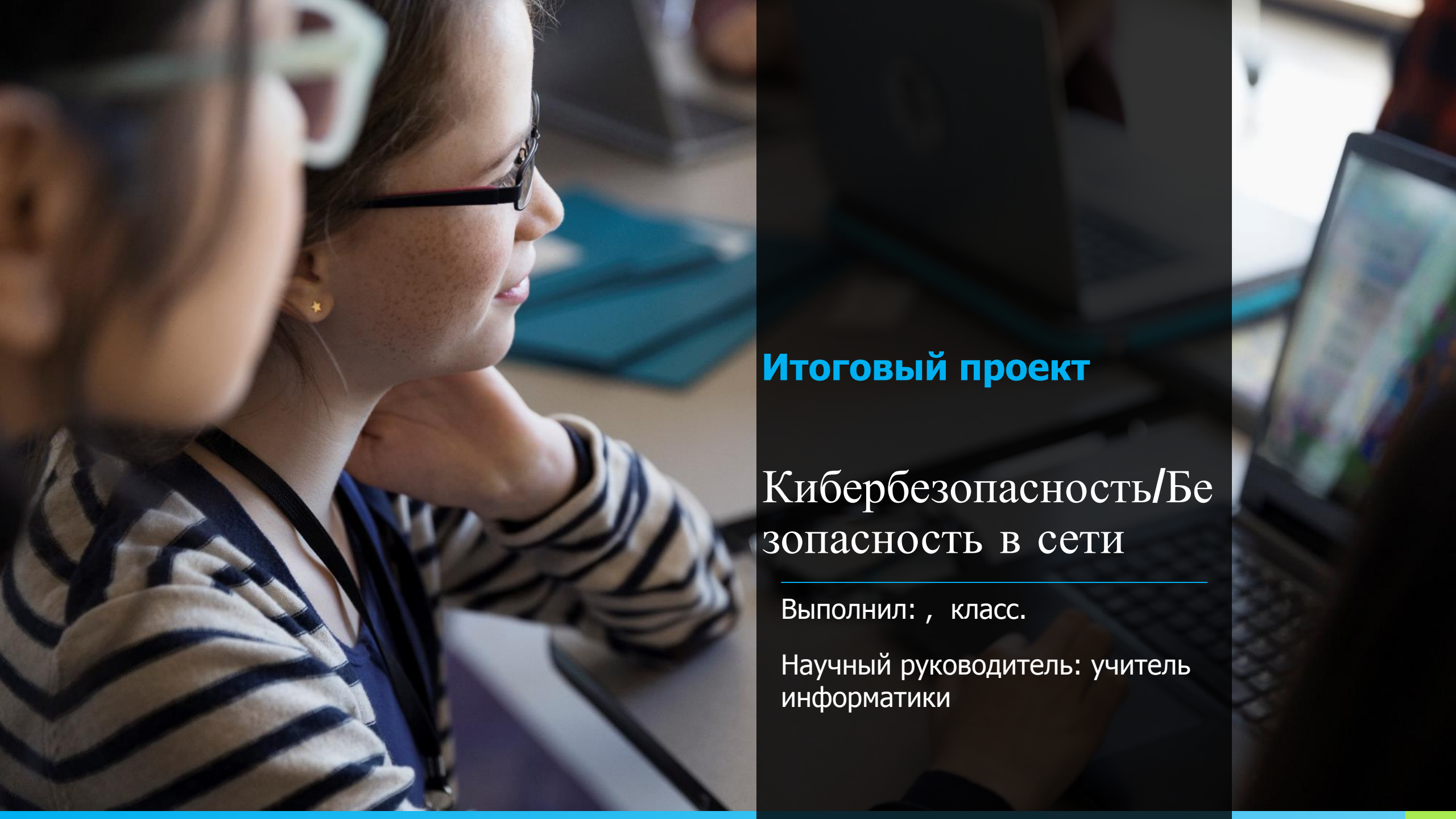


Итоговый проект

Кибербезопасность/Безопасность в сети

Выполнил: , класс.

Научный руководитель: учитель информатики

Введение

Актуальность моей работы: Первоочередная проблема сегодняшнего дня. Она затрагивает пользователей всех возрастов, от детей до людей преклонного возраста. Её актуальность растёт в результате появления большого числа пользователей без первоначальных навыков и умений в сфере IT-безопасности.

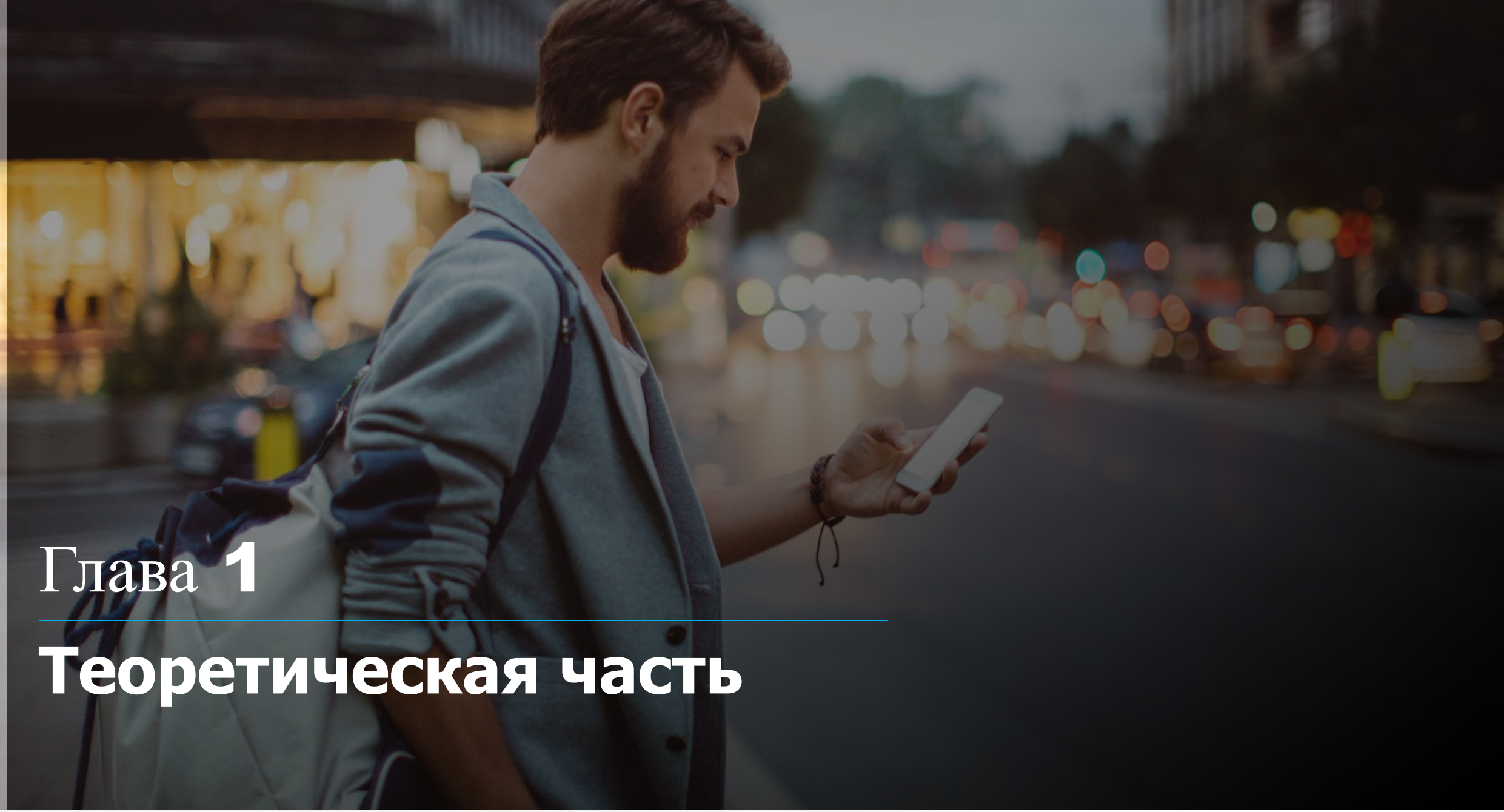
Цель работы: создать инструкцию для повышения уровня безопасности людей, пользующихся интернетом

Задачи:

1. Собрать материалы для исследования.
2. Провести опрос на классном часе.
3. Составить буклет.
4. Анкетировать учащихся.
5. Сделать вывод.

Объект изучения:
процесс выявления опасностей в интернете.
Предмет:
Информатика.

Гипотеза исследования: защищённость компьютеров и их пользователей увеличится, если люди будут больше знать об опасностях интернета.



Глава 1

Теоретическая часть

Понятие компьютерных преступлений

Компьютерные преступления — это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и средством совершения преступления.

- Сложно выявить;
- Трудно предотвратить и нейтрализовать;
- Затруднительно выявить преступников.

Преступники в области информационных технологий – это не только высококвалифицированные специалисты в области компьютерной техники и программирования, но обычные пользователи ПК.

Основные разновидности киберпреступлений

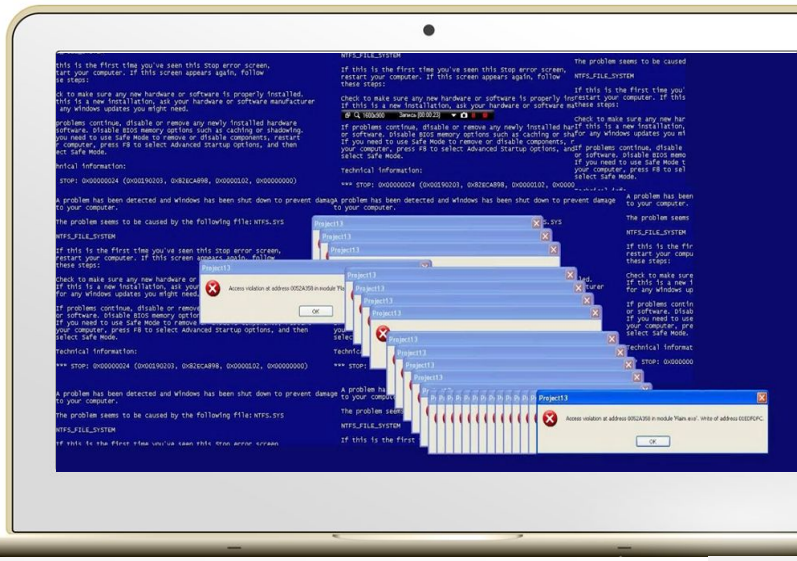
Фишинг

Компьютерные вирусы

Киберпреследование

Кибервымогательство

Кибервойны



Опасности в Интернете

Опасности в Интернете можно разделить на несколько групп:

- **Контентные опасности;**
- **Коммуникационные опасности;**
- **Интернет-мошенничество.**

Наиболее типичные схемы обмана наивных пользователей:

- Потребительское мошенничество;
- Фишинг;
- Интернет-попрошайшничество;
- Обманные знакомства в соц.сетях.

Экстремизм, распространение наркотиков в Интернете

Информационный экстремизм – деятельность, направленная на социально-психическое деструктивное воздействие граждан через использование информационных технологий для достижения противоправных целей. **Признаком** информационного экстремизма является нанесение морального, физического и материального ущерба в результате нарушения законных интересов, прав и свобод граждан.

Незаконный оборот наркотиков и злоупотребление ими продолжают развиваться с нарастающими темпами, представляя серьезную угрозу национальной безопасности нашей страны. Сейчас незаконный оборот наркотиков посредством сети Интернет совершается очень продуманными схемами преступной деятельности. Уровень профессионализма участников растет с каждым днем.

- Антисоциальность;
- Радикальность в действиях;
- Аморальность;
- Противоправность;
- Информационный экстр характер.

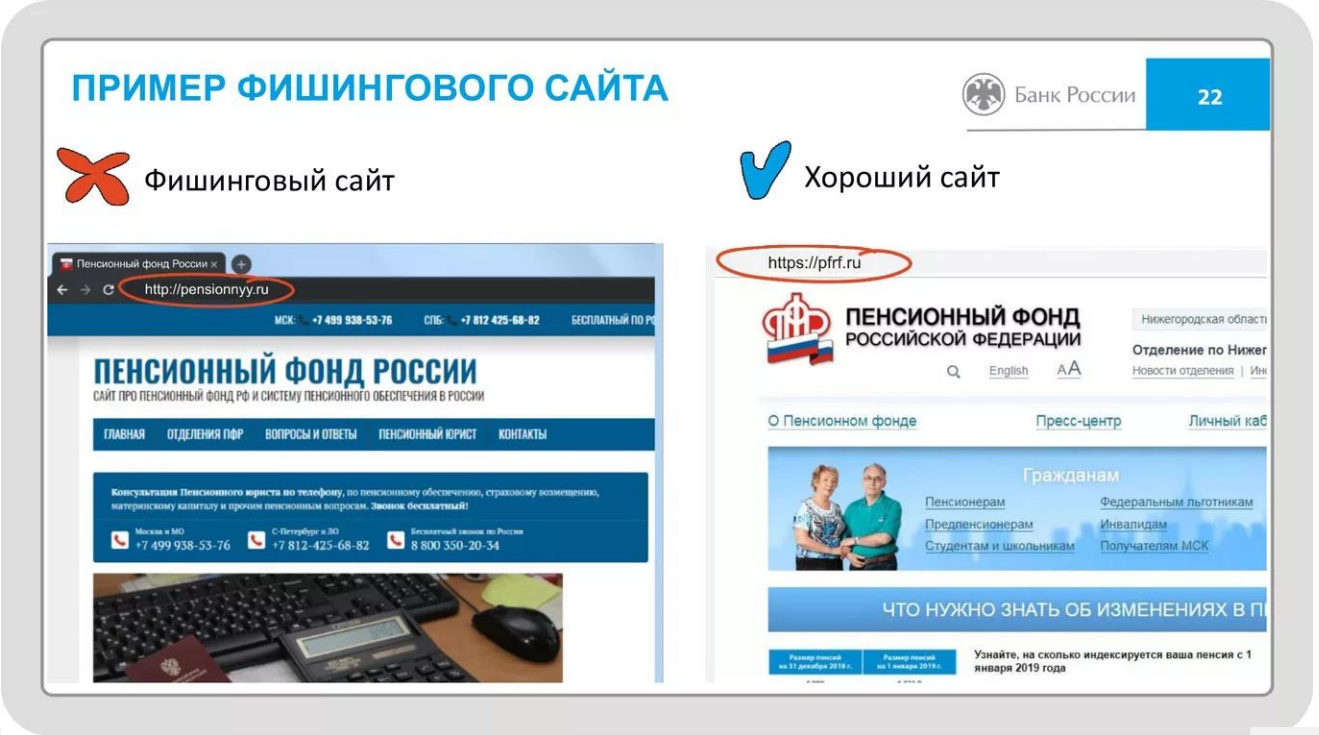
Правоохранительные органы **не могут отслеживать** координационные указания организаторов незаконного оборота, в свою очередь это затрудняет получение информации, которая на стадии предварительного и судебного следствия могла бы стать ключевым доказательством причастности лиц к преступной деятельности.

Фишинг

В основном воруются такие данные:

1. Имя, никнейм, адрес проживания пользователя.
2. Пароли, логины от почты и социальных сетей.
3. Номера телефона, банковского счёта.
4. Данные банковской карточки, её номер, CCV-код, PIN-код.
5. Номер социальной страховки.

Чтобы убедиться в том, что перед вами фишинговый сайт, нужно посмотреть на название сайта в адресной строке браузера. Если оно отличается от оригинального названия сайта, то это фишинговый сайт. Также можно ввести любой придуманный адрес электронной почты и случайный набор символов в качестве пароля.



Советы по защите своей личной информации

Не доверяйте доступ к почте. Она даёт доступ ко многой информации.

Пользуйтесь двухфакторной аутентификацией.

Используйте несколько аккаунтов/почт, пароли тоже должны быть разными и сложными.

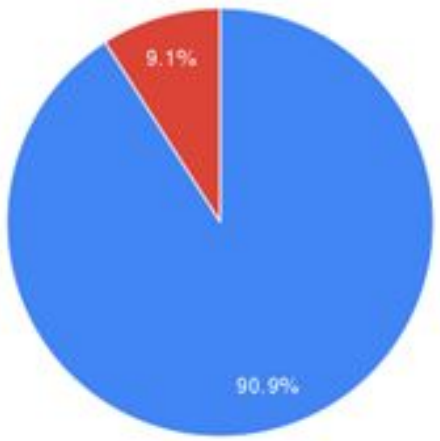
Всегда копируйте свою информацию и имейте резервную копию.

Не доверяйте незнакомым людям и не делайте в Интернете то, что не сделали бы в жизни.

Поддерживайте свою киберграмотность и пользуйтесь антивирусом.

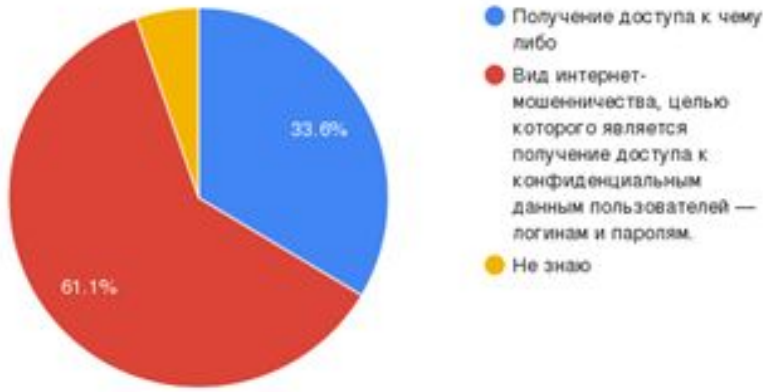
Глава 2

Практическая часть



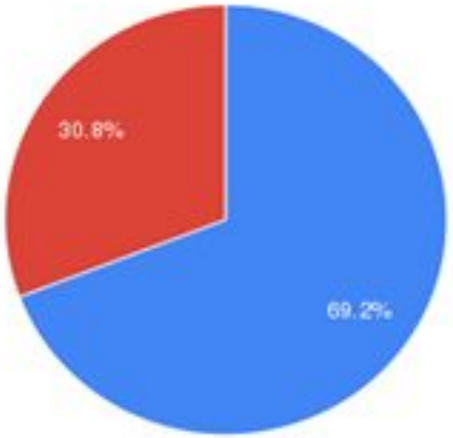
Вопрос 1

Вопрос 2

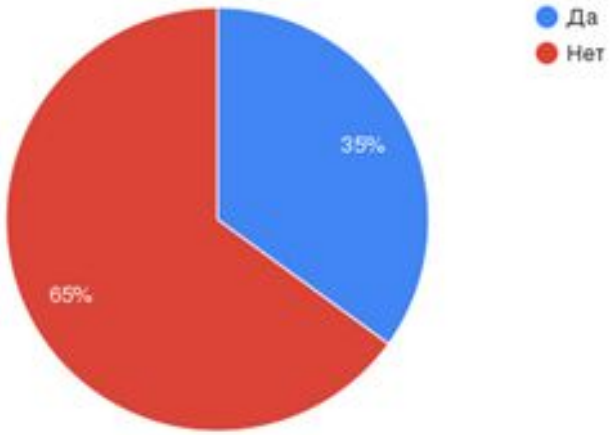


Вопрос 3

3. Как думаешь, что такое фишинг?



Вопрос 4



Вопрос 5

Заключение

Цель проекта я выполнил, после проведения классного часа мои одноклассники узнали, как защитить свою информацию, и практически все ответили на тест правильно. Гипотеза мною также была доказана. На классном часе они узнали, как защитить себя и свой компьютер, и я думаю, что они будут пользоваться этими знаниями в жизни.

Эта тема будет актуальна всегда, так как постоянно будут появляться новые способы обмана людей, но на данный момент я считаю, что при изучении этой темы никаких вопросов у меня не появилось.

Список использованной литературы

1. https://ru.wikipedia.org/wiki/Информационная_безопасность
2. https://pirit.biz/reshenija/informacionnaja-bezopasnost
3. https://mcs.mail.ru/blog/informacionnaya-bezopasnost-i-kakie-dannye-ona-ohranyaet
4. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/
5. http://www.unn.ru/books/met_files/infbezop.pdf
6. https://habr.com/ru/company/vps_house/blog/343110/