МУНИЦИПАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА 147»
Г. НОВОСИБИРСК

Проект

Информационная безопасность в современном интернете.

Выполнил
Степанов Георгий Алексеевич
Учащийся 11 класса

Новосибирск
2022

Оглавление

Введение

- Цель работы: рассмотреть проблемы информационной безопасности, и возможные способы применения современных методов и средств защиты информационных ресурсов.
- Задачи работы:
- 1.Изучить литературу по компьютерной безопасности.
- 2.Выявить проблемы информационной безопасности.
- 3.Изучить правовое регулирование защиты информации.
- 4.Проанализировать пути решения этих проблем.
- 5.Провести анонимное анкетирование среди одноклассников, на основе которого сделать вывод о том, насколько они осведомлены в вопросах, связанных с информационной безопасностью.

Информационная безопасность

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная, или например, физическая).

В основе информационной безопасности лежит обеспечение трех свойств: конфиденциальности, целостности и доступности информации. И обеспечивается это следующими методами:

Программно-аппаратными - сюда входят антивирусы, межсетевые экраны, средства предотвращения утечек информации (DLP-системы), системы обнаружения вторжений, системы управления информацией и событиями в безопасности (SIEM), системы защиты от несанкционированного доступа и т.д.

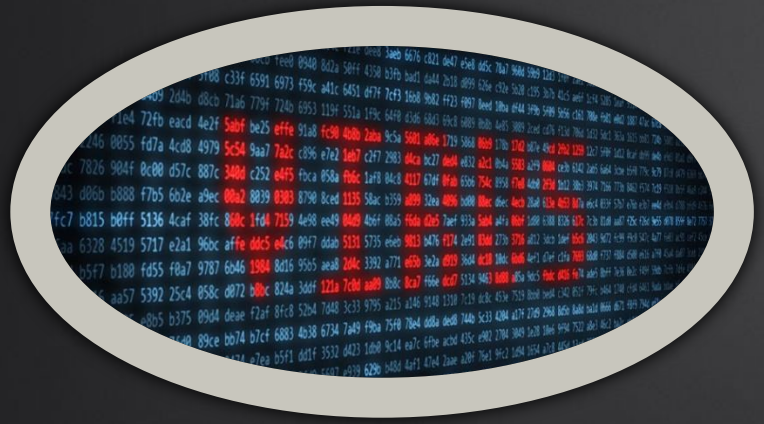
Организационно-правовыми – все, что касается законодательства, нормативной базы и организации работы с информацией.

Техническими - сюда относится зашумление (акустическое и электромагнитное), экранирование, преобразование одних сигналов в другие и иные вещи, тесно связанные с физикой.

Физическими - сюда входят технические средства охраны (видеокамеры, сигнализация) и физические средства защиты (замки, двери, стены)

Криптографические и стеганографические - криптография скрывает смысл сообщения, стеганография скрывает факт передачи сообщения (как Ленин молоком писал). Сюда же относится электронная подпись.

Компьютерные вирусы



- **Компьютерные вирусы** – специально написанные программы, способные самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.
- В настоящее время насчитывается несколько тысяч различных вирусов, и их количество продолжает возрастать. Например, только в глобальной сети Internet ежемесячно появляются не менее 200 вирусов.

Защита от вирусов

- **Антивирусная программа** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Мошенничество и кража в интернете

Данная разновидность мошенничества является наиболее опасной и серьезной, поскольку в сети зарегистрировано огромное количество людей и преступления могут совершаться на дальних расстояниях.

Данный вид преступления представляет собой манипуляции по похищению чужого имущества, осуществляемые путем обманных действий.

Интересные факты

При ограблении банка потери в среднем составляют 19 тысян долларов, а при компьютерном преступлении - 560 тысяч долларов.

По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год и составляет около 3.5 миллиардов долларов.

Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка - и даже при поимке у него меньше шансов попасть в тюрьму.

Обнаруживается в среднем 1 процент компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, меньше 10 процентов.

Опасности в социальных сетях

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Раньше это понятие называлось троллингом. Но суть от этого не изменилась.

Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Основные советы по борьбе с кибербуллингом:

Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

Управляй своей киберрепутацией;

Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

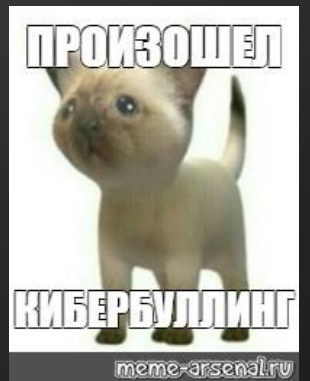
Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно

Соблюдай свой виртуальную честь смолоду;

Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

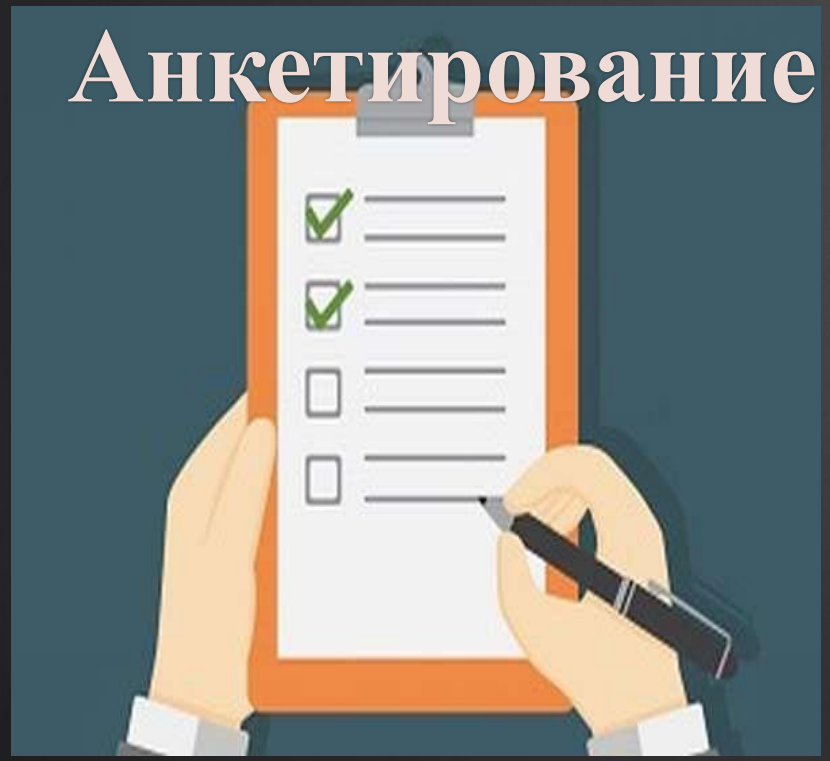


Взлом электронной почты и аккаунтов в социальных сетях

- Как работают хакеры, и как у них получается, регулярно взламывать почтовые ящики известных личностей? Этим вопросом наверняка задаются все, кто читает новости про успешные хакерские атаки.
- Чаще всего взлом почты и аккаунтов в соцсетях происходит из-за неправильно подобранного пароля. Он слишком простой и его легко подобрать. Поэтому нужно правильно его составлять на основе приведенных ниже рекомендаций.

Каким образом лучше выбирать составляющие для пароля?

- Не применять пароль, который является словарным словом. Если есть возможность, то можно использовать знаки препинания. Можно применять символы из нижнего и верхнего регистров, а так же цифры от 0 до 9. Оптимальным для составления пароля является количество цифр (букв) от 8 до 10. Использовать последние символы из списка цифр, знаков или алфавита. Существуют также специальные программы, подбирающие пароли к аккаунту в почтовом сервисе в автоматическом режиме.



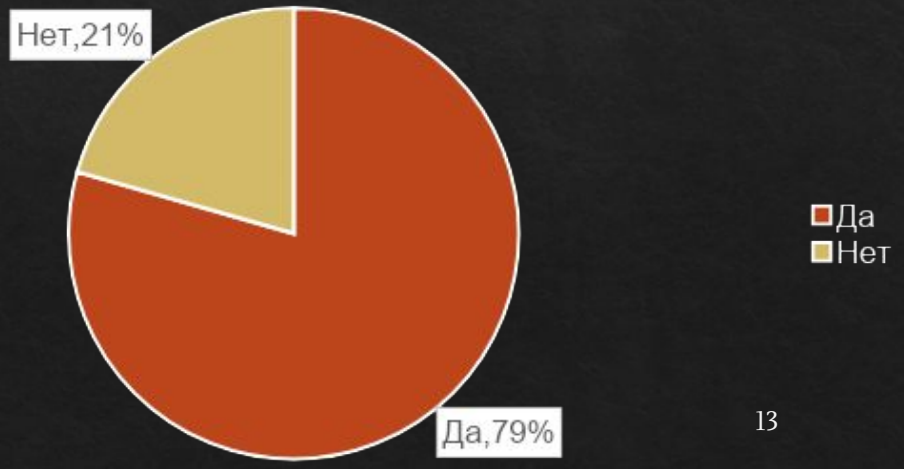
- Выполняете ли Вы правила безопасной работы на компьютере?
- Как Вы считаете, что является информационной безопасностью в современном мире?
- Какой антивирусной программой Вы пользуетесь?
- Сталкивались ли Вы когда - нибудь с компьютерными вирусами?
- Какие аккаунты у Вас взламывали злоумышленники?
- Установлена ли на вашем компьютере программа-фильтр, недопускающая Вас на вредоносные сайты?
- Что Вы делаете, когда приходит предложение о добавлении в «друзья» от незнакомых людей?
- Контролируют ли родители Вашу деятельность в сети интернет?

Выполняете ли Вы правила безопасной работы на компьютере?

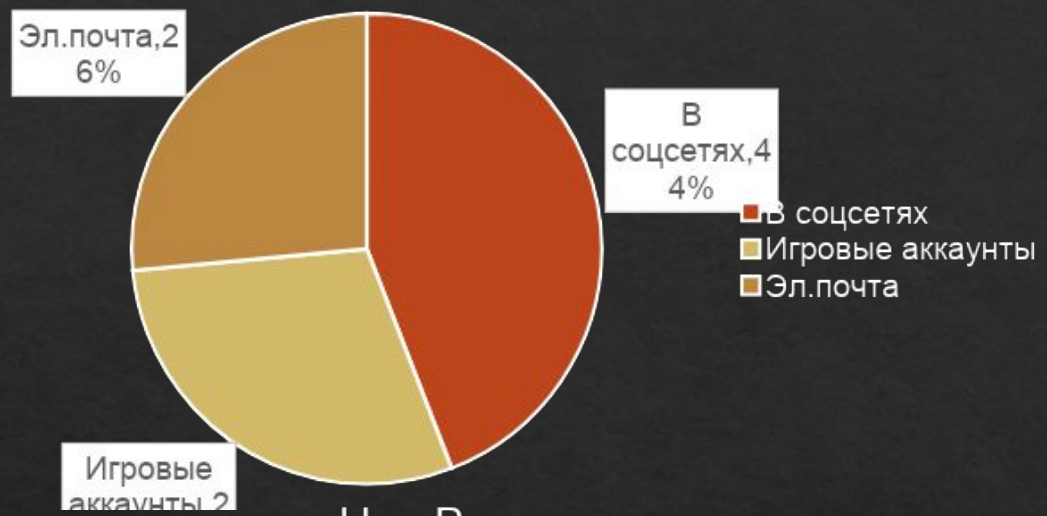
Как Вы считаете, что является информационной безопасностью в современном мире?

Какой антивирусной программой Вы пользуетесь?

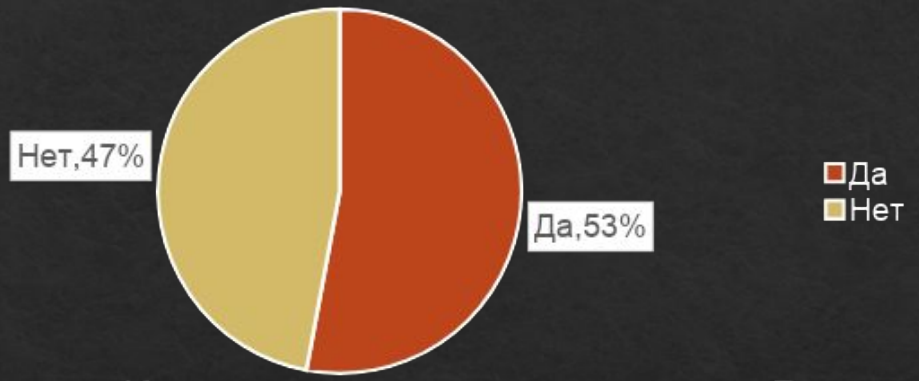
Сталкивались ли Вы когда - нибудь с компьютерными вирусами?



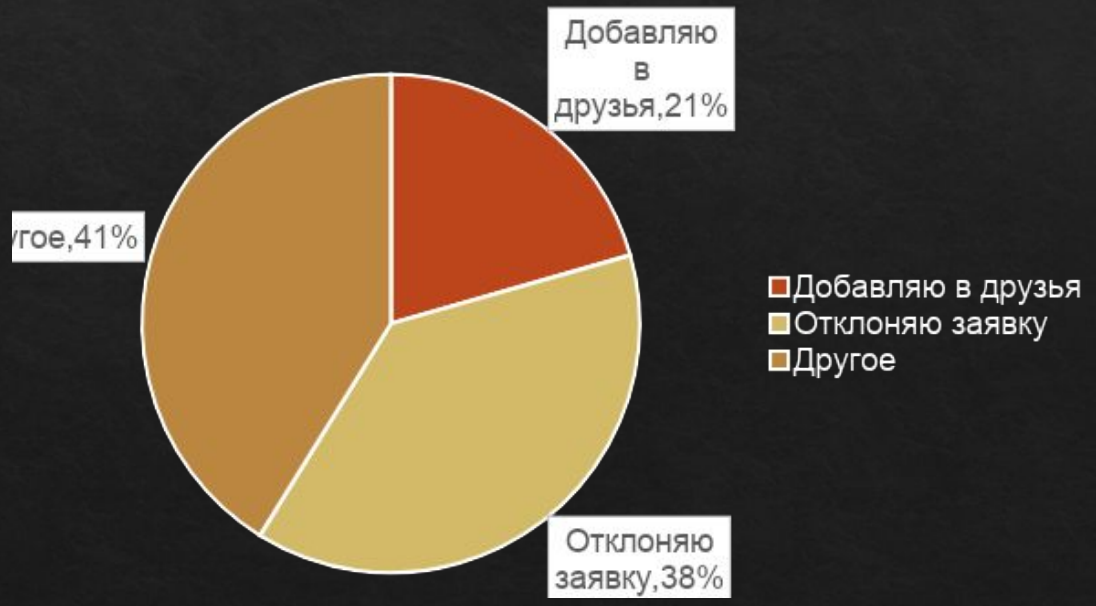
Какие аккаунты у Вас взламывали злоумышленники?



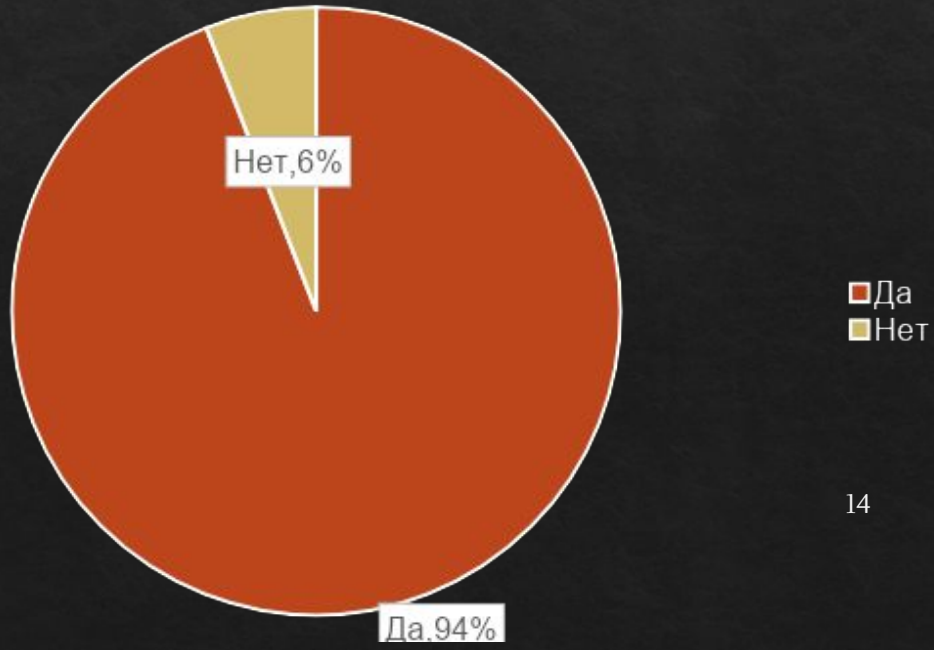
Установлена ли на вашем компьютере программа-фильтр, недопускающая Вас на вредоносные сайты?



Что Вы делаете, когда приходит предложение о добавлении в «друзья» от незнакомых людей?



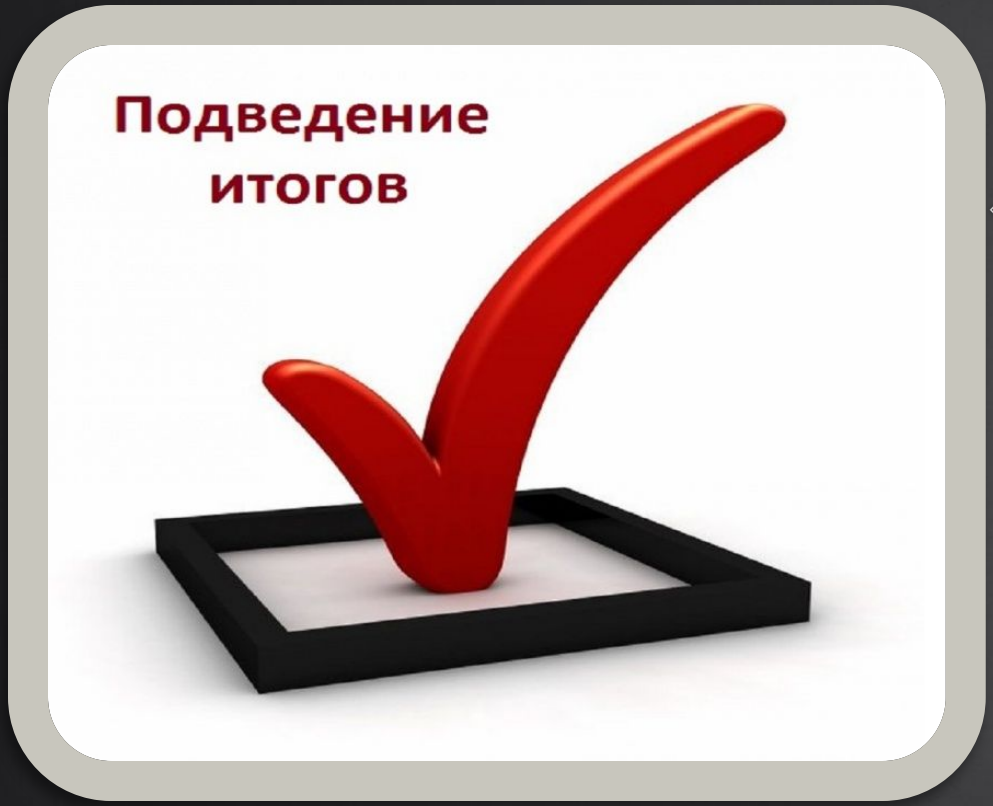
.Контролируют ли родители Вашу деятельность в сети интернет?



Проанализировав информацию, полученную при анкетировании, я могу сказать следующее: опрос показал средний уровень компетентности подростков в вопросах,

Результаты анкетирования:

Проанализировав информацию, полученную при анкетировании, я могу сказать следующее: опрос показал средний уровень компетентности подростков в вопросах, связанных с информационной безопасностью в сети интернет.



- Заключение: Данный проект помог узнать мне много необходимого о компьютерной безопасности, проведя анкетирование я узнал, что ребята моей возрастной группы осведомлены о безопасности в интернете.Мой проект должен дать знания и отгородить от взломов и краже средств его слушателей.

Книги:

Белов Е. Б., Лось В. П. Основы информационной безопасности.
–М. : Горячая линия : Телеком, 2006. –544 с.

Интернет ресурсы:

http://ligainternet.ru/
http://chopsarmat.ru/articles/informatsionnaya_bezopasnost_detey.html

Спасибо за внимание!