Киберпреступность

Выполнила:
ученица 9 «Г» класса

Руководитель проекта:
Чертаков Дмитрий Ва
учитель предмета
Информатики и ИКТ

Абстракт

- Цель работы:

- изучить проблемы развития киберпреступности в мире и найти способы ее профилактики.

- Актуальность:

выбранная мной тема интересна своей актуальностью, так как почти многие подвергались взломами личных данных.

- Задачи:

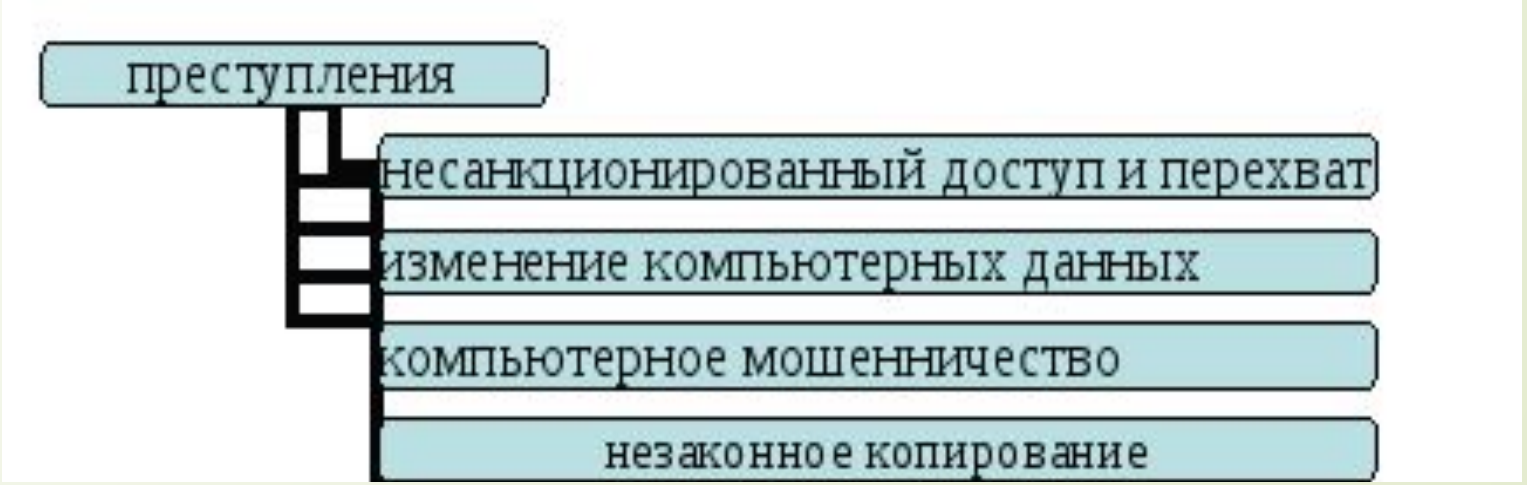
1. Суть киберпреступности.
2. Рассмотреть виды киберпреступлений.
3. Провести опрос в социальных сетях.
4. Дать рекомендации противостоянию хакерам.

Введение.

- Сегодня мы живем и работаем в мире глобальных возможностей взаимодействия. Мы можем вести легкомысленную беседу или совершать многомиллионные денежные операции и сделки с людьми с другой стороны планеты быстро и недорого. Стремительное увеличение количества персональных компьютеров, свободный доступ к Интернету и быстро развивающийся рынок новых коммуникационных устройств изменили и способы проведения досуга, и методы ведения бизнеса. Меняются и способы совершения преступлений.

1.1 Суть и виды киберпреступлений.

- Конвенция Совета Европы о киберпреступности говорит о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:



1.2.Атаки на пользователей.

Количество атак на частных лиц продолжает расти. За 2019 год я насчитала 231 хакерскую кампанию, направленную на обычных пользователей (за аналогичный период 2018 года — 217 компаний). Как правило, это массовые атаки, которые затрагивают одновременно множество жертв, и подсчитать точное их число или масштаб ущерба невозможно. Как и прежде, основными способами добраться до данных пользователей являются социальная инженерия и заражение устройств вредоносным ПО. Преступники продолжают использовать неграмотность людей в вопросах обеспечения собственной информационной безопасности.

1.3. Примеры и анализ наиболее крупных кибератак.

1.4. Мошенничество с финансовыми ресурсами с использованием компьютерных технологий и информационнокоммуникационных систем.

- В рамках данного исследования, под кибермошенничеством понимается мошенничество, совершенное с использованием компьютеров, компьютерных сетей, информационно-коммуникационных систем и сети Интернет. Мошенники так же используют современные возможности сети Интернет для своих махинаций. Достаточно распространенными являются:

1.5. Мошенничество в системах дистанционного банковского обслуживания.

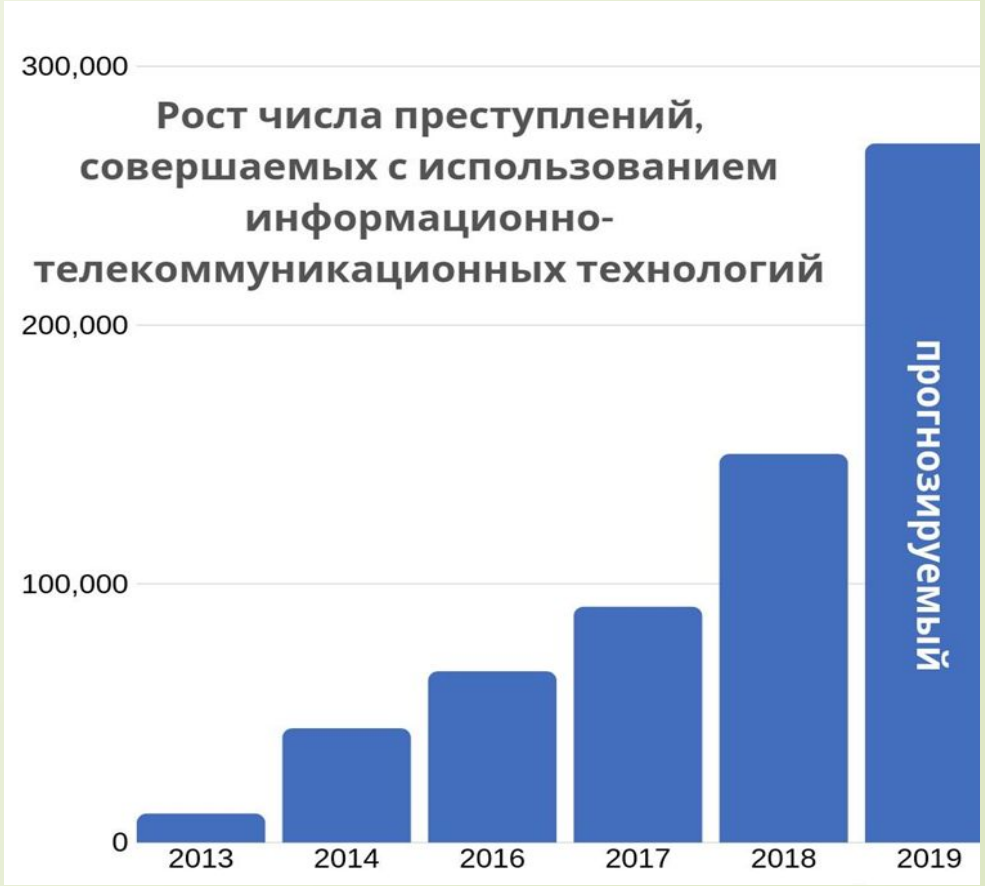
- В современных условиях системы ДБО (Клиент-Банк, Интернет-КлиентБанк, Интернет-банкинг и т.п.) стали неотъемлемой частью финансовой системы во всем мireИспользование системы ДБО, бесспорно, имеет свои преимущества. Прежде всего следует выделить следующие:
-

1.6. Законодательство РФ в сфере информационной безопасности.

- В области информационной безопасности Российской Федерации существуют следующие нормативные документы:
- Закон РФ «О правовой охране ЭВМ и баз данных»;
- Доктрина информационной безопасности РФ;
- Уголовный кодекс РФ;

2.1.Опрос и выводы.

За последние 6 лет число преступлений, совершаемых с использованием современныхинформационно-телекоммуникационных технологий, выросло в 25 раз. К концу 2019 года доля таких правонарушений от общего числа зарегистрированных преступлений за год составит не менее 14%. Это порядка 270 000 зарегистрированных преступлений.

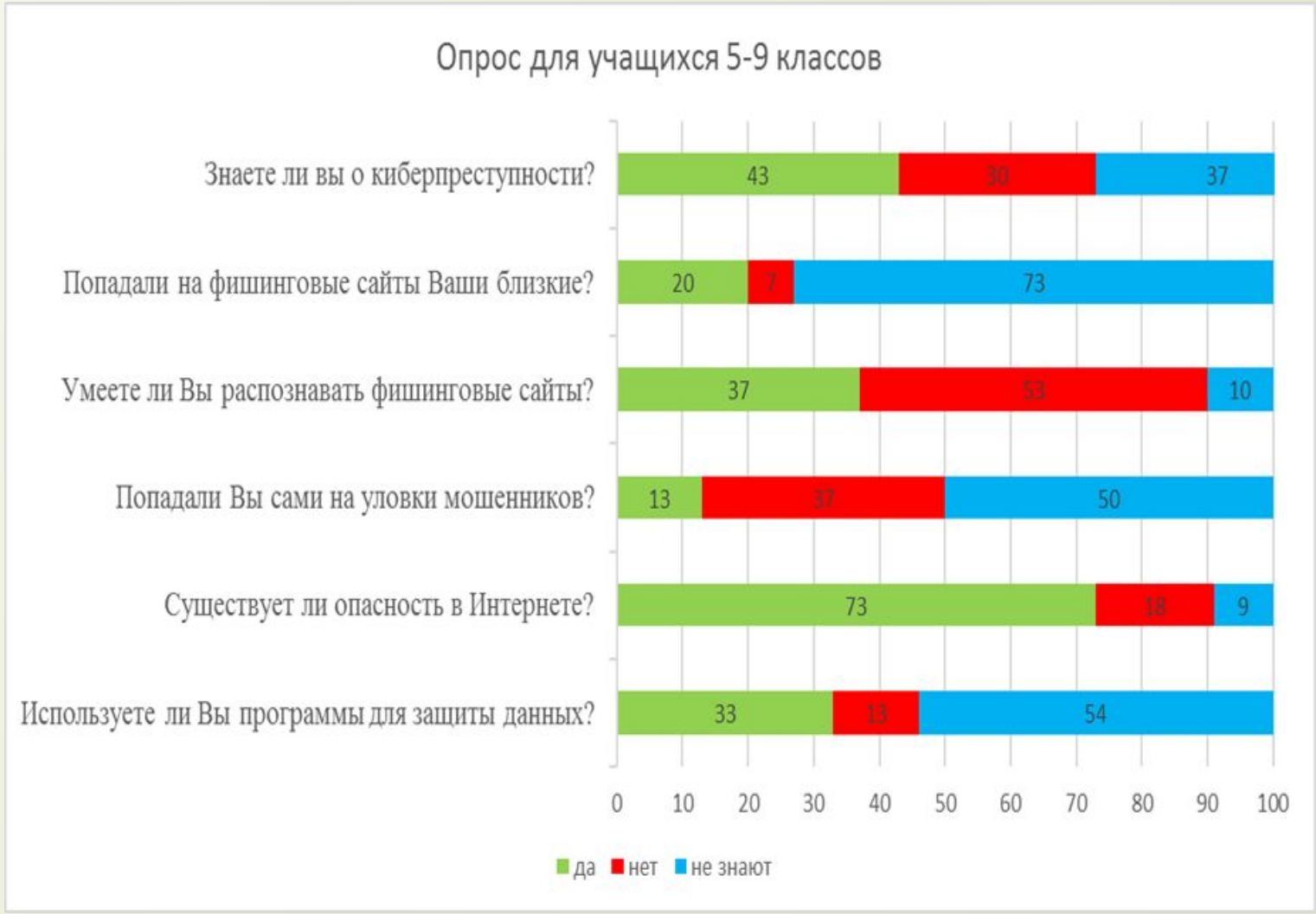


2.1.Собственное исследование.

- Для подготовки данной исследовательской работы мной был проведен интернет-опрос среди учеников нашей школы, благодаря которому я узнала, что больше половины опрошенных уверены, что в интернете для них существует опасность, и почти все используют различные элементарные правила безопасности в сети. По результатам видно, что 64% опрошенных знают, что такое киберпреступность, и те же 64% сталкивались с ней в интернете. Самыми распространёнными видами, судя по результатам опроса, являются спамерство и хакерство.

2.1 Опрос и выводы

- В опросе для учащихся 5-9 классов замечено, что они меньше знают про киберпреступность, так как по программе они еще не начинают говорить про киберпрострнство и из этого следует, что они меньше осведомлены, и больше вероятности того,что они не знают как предотвратить взлом.



2.1 Опрос и выводы

- В опросе для учащихся с 10-11 класс замечено, что они больше знают про киберпреступность,так как в 10-11 классов уже прошли киберпротванство и уже начинают проходить шифрование,чем в 5-9 классах. Из этого следует, что они больше знают как обезопасить себя от взлома.

2.2.Первоочередные шаги для повышения безопасности.

- 1. Регулярно скачивайте обновления для программного обеспечения часть атак идёт через неисправленные ошибки.
- 2. Настройте межсетевой экран для фильтрации нежелательных входящих
- соединений.
- 3. Установите качественное антивирусное и антишпионское программное
- обеспечение.
- 4. Установите спам-фильтр в почтовые программы (например, в Outlook)
- Не открывайте писем от пользователей, которых вы не знаете.
- 5. Не переходите по ссылкам на неизвестные сайты (соц.сети, банки, интернет-магазины) непосредственно из писем. Очень часто такие письма являются фишинговыми. Часто посещаемые сайты лучше держать в браузере в закладках. Ну или каждый раз искать эти сайты в яндексе, гугле.
- 6. Придумывайте (возможно, с помощью специальных генераторов) надёжные не повторяющиеся пароли.
- 7. Храните несколько резервных копий важных данных.
- 8. Обращайте внимание, если ваши знакомые начинают вести себя необычно игнорируйте их просьбы одолжить денег или предоставить другие ресурсы. Лучше уточнить подробности по телефону или лично.

2.3.ВЫВОДЫ.

- Несмотря на отсутствие на сегодня общепринятого определения киберпреступления наблюдается достаточно широкое и исчерпывающее понимание его сути и способов его совершения, а также угроз и рисков, что дает возможность разрабатывать и внедрять меры противодействия данному виду преступления. Отсутствие физического контакта с жертвой или представителями финансового учреждения, а также анонимность, скорость осуществления и невысокая стоимость преступления стали ключевыми предпосылками повышения заинтересованности преступников киберпространством.