«ВЛИЯНИЕ КИБЕРБЕЗОПАСНОСТИ НА ИНФОРМАЦИОННУЮ ЖИЗНЬ ОБЩЕСТВА».

Исполнитель: учащаяся 10Б класса

МБОУ ТЭЛ

Усольцева Даниэлла

Руководитель: учитель информатики

Татенко Е.В.

ВВЕДЕНИЕ

Цель: Выявить влияние кибербезопасности на информационную жизнь общества.

Задачи:

1. Изучить, что такое кибербезопасность.
2. Проанализировать найденную информацию.
3. Изучить распространение киберпреступлений за 4 года.
4. Выяснить возможные варианты сокращения киберпреступности и улучшение кибербезопасности в интеренете.
5. Сделать вывод по теме.

КИБЕРБЕЗОПАСНОСТЬ И КИБЕРУГРОЗА

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий. Из-за плохой кибербезопасности возникают киберугрозы.

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

ВИДЫ КИБЕРУГРОЗ

1. **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
3. **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

РАЗДЕЛ ЗАРАЖЕНИЕ И ИНФОРМАЦИЯ О НЕМ.

Вредоносное ПО так же относится к виду киберугроз рассмотрим их поподробней. Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

ВРЕДОНОСНОЕ ПО МОЖЕТ БЫТЬ САМЫМ РАЗНЫМ, ВОТ НЕКОТОРЫЕ РАСПРОСТРАНЕННЫЕ ВИДЫ:

1. **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
2. **Троянцы–** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
3. **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
4. **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
5. **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
6. **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

ВРЕДОНОСНЫЕ ПРОГРАММЫ

- В 1994 году AV Test зарегистрировал в своей базе данных всего 28 613 уникальных вредоносных программ. К 2005 году компания сообщила, что ее база данных выросла до 333 425. Это увеличение на 1100% всего за 10 лет.
- К 2007 году ее база данных выросла до более чем 5 миллионов зарегистрированных вредоносных программ.
- В 2014 году несколько фирм, отслеживающих развитие вредоносных программ и регистрирующих вредоносные программы, показали, что ежедневно обнар уживается до 500 тыс. Новых вредоносных программ.

УЩЕРБ ОТ КИБЕРПРЕСТУПЛЕНИЙ

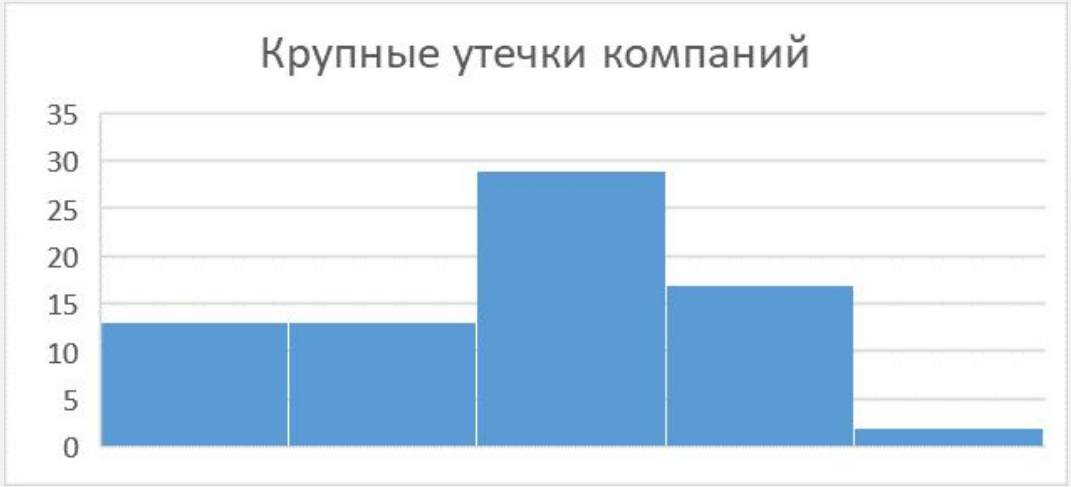
По данным **Фонда "Общественное мнение"**, на осень 2012 года месячная аудитория Интернета в России составляла 61,2 млн человек старше 18 лет, что составляет более 52% всего совершеннолетнего населения страны. Для большинства пользователей Интернет стал повседневным, привычным явлением. Три четверти выходящих в сеть (почти 47 млн человек) делают это ежедневно. По данным **TNS** в городах с населением более 100 000 жителей у 94% пользователей есть выход в сеть из дома. Интернет-аудитория по-прежнему растет, хотя темпы роста несколько замедляются – с осени 2010 года по осень 2011 года она увеличилась на 17%, а с 2011 года по 2012 год рост составил 12%. Анализ базы данных интернета за 2011 год показал следующие результаты (рис.1).

По данным Norton Cybercrime Report 2012 каждый пятый человек старше 18 лет становился жертвой кибератаки либо в социальных сетях, либо через мобильные устройства. Большинство пользователей Интернета предпринимают лишь базовые действия по защите информации (удаляют подозрительные электронные письма, с осторожностью раскрывают личные данные), однако не обращают внимания на такую важную меру, как создание сложных паролей и их регулярное изменение.

КРУПНЫЕ КИБЕРПРЕСТУПЛЕНИЯ

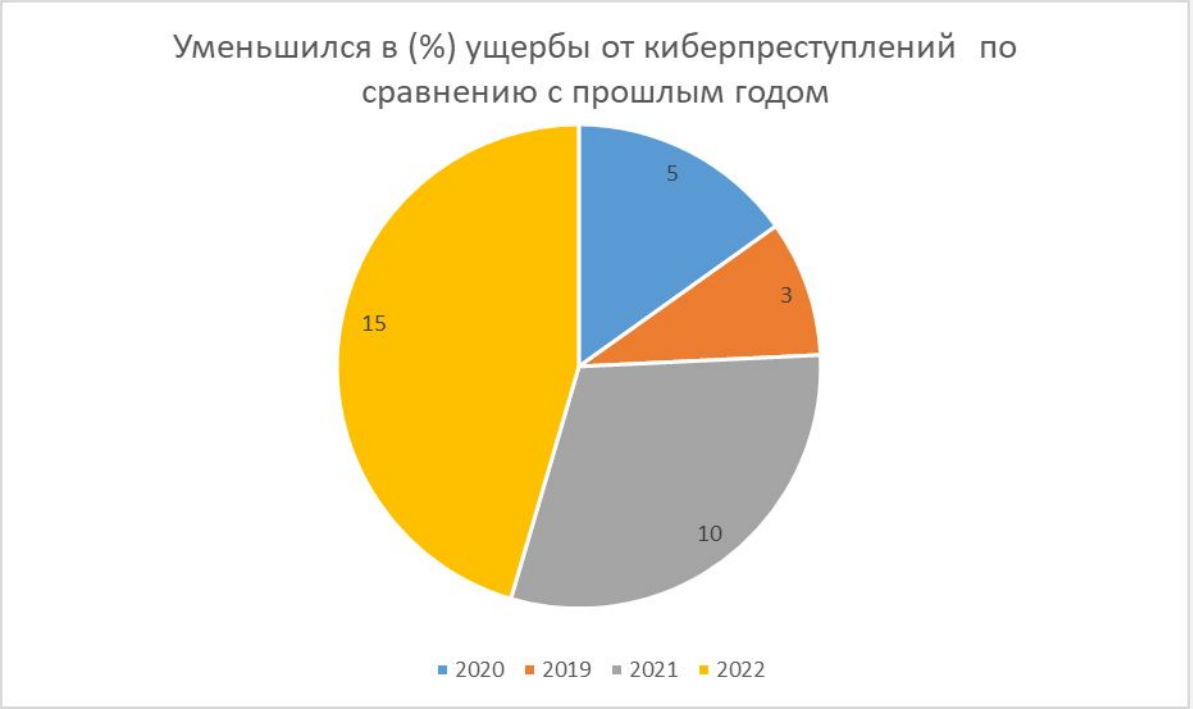
Достаточно взглянуть на несколько утечек данных, произошедших с 2005 года, взятых из подробной инфографики, предоставленной Slate :

- AOL (скомпрометировано 92 миллиона записей)
- Citigroup (3,5 миллиона скомпрометированных записей)
- TJ Maxx (скомпрометировано 94 миллиона записей)
- Военные США (скомпрометировано 76 миллионов записей)
- TD Ameritrade (скомпрометировано 6,3 миллиона записей)
- Heartland (скомпрометировано 130 миллионов записей)
- Sony Playstation Network (скомпрометировано 77 миллионов записей)
- Blizzard Entertainment (скомпрометировано 14 миллионов записей)
- Apple (скомпрометировано 12,3 миллиона записей)
- Evernote (скомпрометировано 50 миллионов записей)
- Живое общение (скомпрометировано 50 миллионов записей)
- Yahoo (скомпрометировано 22 миллиона записей)
- Facebook (скомпрометировано 6 миллионов записей)



МОЕ ИССЛЕДОВАНИЕ

Я провела исследование по ущербам от киберпреступлений в минувшие 4 года. Ущерб от кибепреступлений в 2019 году уменьшился на 3%, по данным 2020 года уменьшился на 5%. В 2021 году ущерб уменьшился на 10%, а в 2022 на 15%. С каждым годом ущербы от киберпреступлений уменьшались, это говорит о развитии кибербезопасности в нашей стране. Начиная с 2000 года и до недавнего времени ситуация киберпреступлений ухудшалась, ущербы становились неподъемными и давили на экономику страны. Ежегодно многомиллиардные средства выделялись на погашение ущербов, что сказывалось на бюджете страны. А значит на каждом из проживающих в стране. Но после развития кибербезопасности все пришло в норму, и с каждым годом ситуация радует все больше.



СПОСОБЫ УЛУЧШЕНИЯ КИБЕРБЕЗОПАСНОСТИ.

1. Разработки и внедрения механизма двойной проверки платежей, которые позволяют банкам возвращать в полном объёме деньги, которые похитили мошенники. Для этого регулятор настаивает на внесении изменений в статью закона «О национальной платёжной системе». Двойную проверку подозрительных операций с деньгами будут инициировать банки отправителя и получателя.
2. Нулевое доверие (Zero Trust) – модель безопасности, предполагающая, что любая транзакция, пользователь или устройство являются несакционированными до тех пор, пока не доказано обратное. Причем достоверность транзакции, пользователя или устройства должна подтверждаться вновь и вновь.
3. Внедрение курсов для обучения правоохранительным органов в сфере IT.
4. Ознакомление людей с новыми прогрессирующими формами киберпреступлений.

ЗАКЛЮЧЕНИЕ

Я смогла выполнить поставленные задачи и сделала определенный вывод. Одна вещь, которая примечательна в эволюции кибербезопасности. В течение многих лет индустрия занимала ответственную позицию, устраняя угрозы по мере их возникновения и создавая исправления для вирусов и вредоносных программ после их выпуска. После атак нулевого дня и молчания компаний после того, как произошли нарушения, мы видим больший сдвиг в сторону упреждающего подхода к кибербезопасности. Вместо того чтобы ждать атаки или нарушения, организации разрабатывают способы предотвращения угроз и устранения возможностей до того, как атаки могут произойти. После проводимых мной исследований удалось выяснить: с каждым годом ущербы от киберпреступлений уменьшались, это говорит о развитии кибербезопасности в нашей стране. А значит о улучшении уровня жизни.

СПАСИБО ЗА ВНИМАНИЕ!