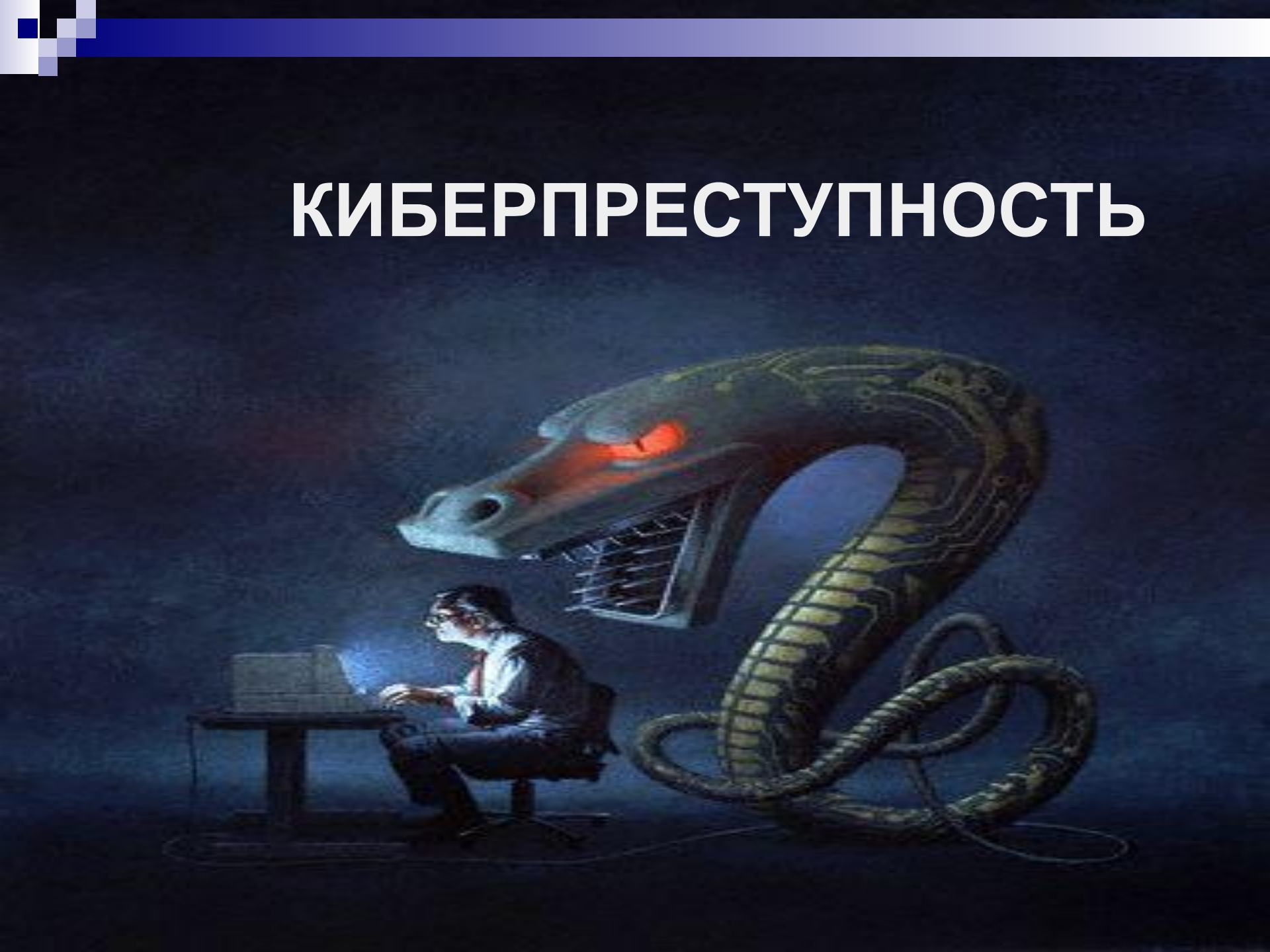
КИБЕРПРЕСТУПНОСТЬ



АБСТРАКТ

- Цели: рассказать о киберпреступности, какие киберпреступления совершаются в мире, какие меры борьбы предпринимаются.
- Задачи: Изучить виды киберпреступности происходящих в мире и в нашей стране.

ГИПОТЕЗА

Знание о киберприступниках и киберпреступлениях необходимо для работы с информацией в современном мире.

- ГЛАВА I - 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. Доступность глобальных цифровых технологий открывает новые возможности недобросовестным лицам. И бизнесмены, и потребители лишились миллионов долларов “с помощью” обладающих компьютерными знаниями преступников. Хуже того, компьютеры и сети могут использоваться для того, чтобы вызвать тревогу, посеять панику ожидания насильственных нападений – и даже для координации и осуществления террористических действий. К сожалению, во многих случаях правоохранительные органы отстают от преступников, испытывая недостаток технологий и квалифицированного персонала для отражения новой и быстро растущей угрозы, названной киберпреступностью.

Киберпреступность

это слово звучит странно, напоминая футуристические научно-фантастические романы. Однако сотрудники правоохранительных органов, сетевые администраторы, имеющие дело с преступностью и/или киберпространством, обнаруживают, что будущее уже наступило, и киберпреступность – проблема.

Практически каждый имеет потенциал для противодействия киберпреступности, но две группы людей должны непосредственно иметь дело с этим явлением по нижеуказанным основаниям:

IT – профессионалы, наиболее часто ответственные за обеспечение первой линии защиты от киберпреступлений и их выявления;

Профессионалы – сотрудники правоохранительных органов, ответственные за решение ставящих в тупик правовых, юрисдикционных и практических вопросов, возникающих при попытке предать киберпреступников суду.

Хотя для успеха в любой войне с киберпреступностью необходимо, чтобы эти две группы работали вместе, зачастую между ними возникают разногласия, поскольку ни у одной стороны нет реального представления о том, что делает другая, и о своих собственных возможностях в процессе борьбы с киберпреступлениями.

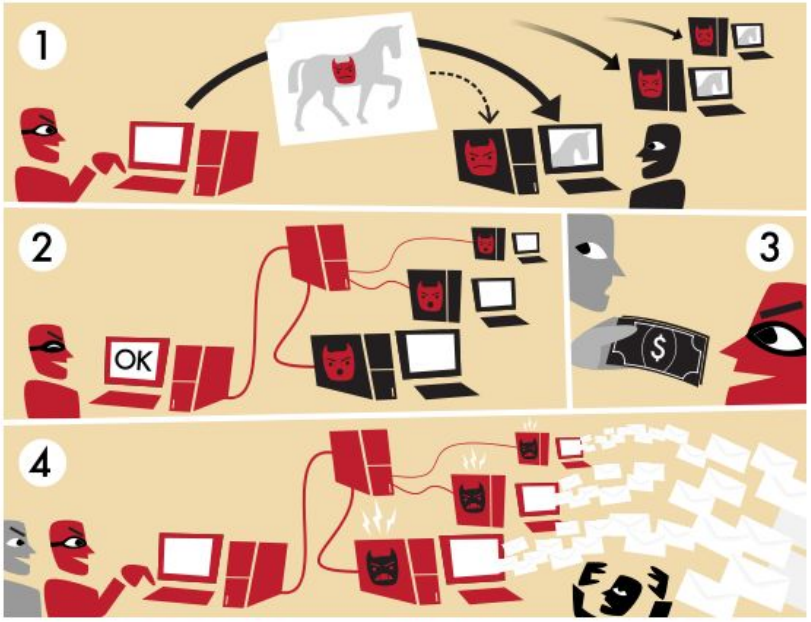
Киберпреступность может определяться как подкатегория компьютерной преступности. Термин подразумевает преступления, совершенные с использованием сети Интернет или иной компьютерной сети, как компонента преступления. Компьютеры или сети могут быть задействованы в совершении преступлений следующими способами:

- ***Компьютер или сеть могут быть инструментом преступления (использоваться для совершения преступления).***
- ***Компьютер или сеть могут быть целью преступления (“жертвой”).***
- ***Компьютер или сеть могут быть использованы для достижения дополнительных целей, которые связанны с преступлением (например, ведение регистрации незаконной продажи наркотиков).***

ОТЛИЧИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ, ОТ ПРЕСТУПЛЕНИЙ, ЗАВИСЯЩИХ ОТ СЕТИ.

Во многих случаях преступления, которые мы можем согласно нашему общему определению назвать “киберпреступлениями” - в действительности уже существуют, за исключением того, что при их совершении так или иначе используется компьютерная сеть. Таким образом, человек мог использовать Интернет для построения финансовых пирамид, рассылки “писем счастья”, привлечения клиентов в притоны, сбора ставок для нелегальных азартных игр. Все эти деяния уже являются незаконными во многих юрисдикциях и могли бы быть совершены без использования компьютерной сети. “Кибер” аспект не является необходимым элементов преступления, а служит лишь средством совершения преступления. Компьютерные сети предоставляют преступникам новые способы совершения “старых” преступлений. Существующие законы, запрещающие подобные действия, могут применяться к лицам, совершившим эти деяния с помощью компьютеров и сетей, точно так же как к тем, кто совершил их без использования новых технологий.

В других случаях преступление является уникальным и обязано своим существованием появлению сети Интернет. В качестве примера можно привести незаконный доступ. Он может быть уподоблен незаконному проникновению в дом или офисное здание, но признаки незаконного компьютерного доступа отличаются от признаков физического взлома. В определении, данном в законах, взлом и проникновение обычно требуют физического входа на территорию помещения, признака, который не представлен в преступлении, произошедшем в киберпространстве. Таким образом, новые законы должны учитывать эту специфику.



Виды киберпреступников.

Фишеры

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Целью фишинга является получение доступа к таким конфиденциальным данным, как номера банковских счетов, PIN-коды и т. п.

Спамеры

Реклама в Интернете является одним из наиболее бурно развивающихся видов рекламы. Ее преимуществами являются минимальные затраты и высокая вероятность непосредственного общения с потребителем.

К спаму относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств для получения новых адресов электронной почты.

Инсайдер— член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер — это член группы, обладающий информацией, имеющейся только у этой группы.

Хакер — чрезвычайно квалифицированный ИТ-специалист, человек, который понимает самые глубины работы компьютерных систем. Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда элегантным или профессиональным способом

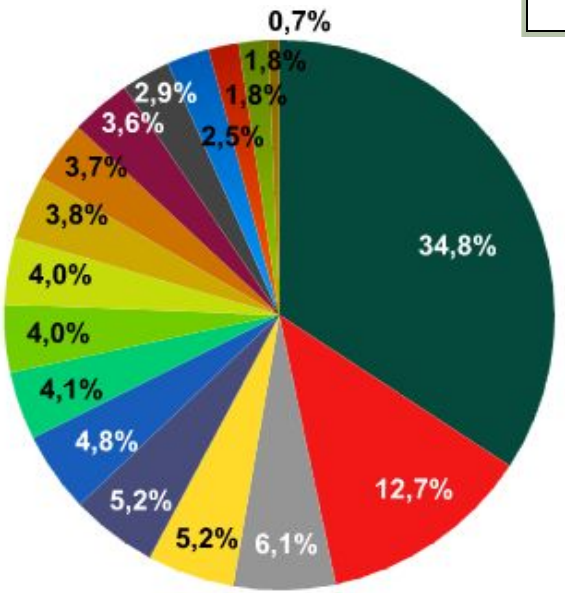
СБОР СТАТИСТИЧЕСКИХ ДАННЫХ ПО КИБЕРПРЕСТУПНОСТИ.

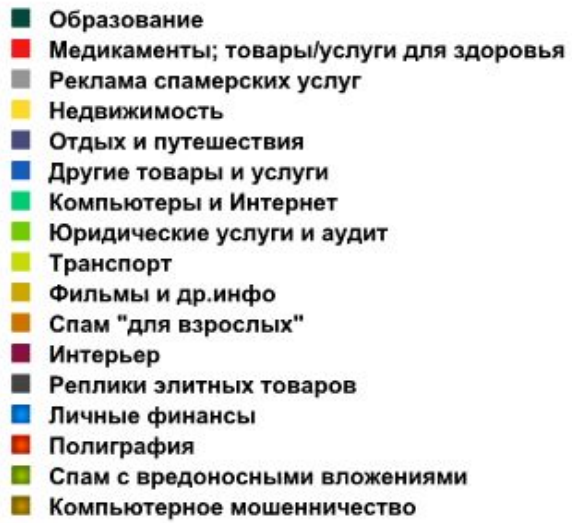
Помимо корректного определения киберпреступности есть еще одна проблема – отсутствие точных статистических данных об этих правонарушениях. Однако сообщение о преступлениях в эти агентства производится на добровольной основе. Это означает, что количество преступлений, о которых сообщают эти агентства, несомненно, намного ниже, чем фактическое их количество. Это не только из-за латентности, когда о неизвестном количестве преступлений не сообщается, но еще и из-за того, что о большинстве преступлений, которые зарегистрированы полицией, не сообщается в агентства, собирающие статистику.

В настоящее время на практике фактически невозможно даже получить данные о точном количестве киберпреступлений, зарегистрированных полицией. Чтобы понять, почему это так, нужно рассмотреть, как собираются данные об этих преступлениях в США.

Типы кибератак

Географическое происхождение кибератак





Структуры, подвергающиеся кибер атакам

МЕЖДУНАРОДНОЕ ПРАВО: ОПРЕДЕЛЕНИЕ КИБЕРПРЕСТУПНОСТИ ООН.

Киберпреступность не знает не только границ штатов, но и государственных границ. Возможно, для выработки наиболее подходящего стандартного определения нам следует обратиться к опыту международных организаций.

На X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями на симпозиуме по проблемам преступлений, связанных с компьютерами и компьютерными сетями, киберпреступления были подразделены на следующие две категории:

- *Киберпреступление в узком смысле (компьютерное преступление): любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных.*
- *Киберпреступление в широком смысле (как преступление, связанное с компьютерами): любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей.*

- Незаконный доступ
- Повреждение (нанесение ущерба) компьютерным данным или программам
- Компьютерная диверсия
- Неправомерный перехват коммуникаций
- Компьютерный шпионаж

Эти определения, не являясь полными, дают нам хорошую отправную точку – поскольку подкреплены международным признанием и соглашениями – для определения того, что мы подразумеваем под термином киберпреступление.

IT – профессионалы нуждаются в хорошем определении киберпреступления, чтобы знать когда (и о чем) сообщать полиции, но правоохранительным органам необходимо законодательное определение этого вида преступлений для привлечения к ответственности правонарушителей. Первый шаг в конкретном определении отдельных киберпреступлений – классификация всех действий, которые могут рассматриваться в качестве киберпреступлений, на упорядоченные категории.

$526

СКОЛЬКО ТЫ СТОИШЬ?

$300 ТЫ ТЕРЯЕШЬ

- **$20** НЕСКОЛЬКО СМС ДЛЯ ПОЛУЧЕНИЯ КОДА РАЗБЛОКИРОВКИ ОС
- **$25** УКРАЛИ АККАУНТ SKYPE С ДЕНЬГАМИ НА СЧЕТУ
- **$45** ТРОЯНЦЫ ОТПРАВЛЯЮТ ДОРОГИЕ СМС НА ПРЕМИУМ-НОМЕРА
- **$100** ВОССТАНОВЛЕНИЕ ДАННЫХ, ЗАШИФРОВАННЫХ ТРОЯНЦЕМ GPCODE
- **$30** СМС-УЧАСТИЕ В БЕЗВЫИГРЫШНЫХ ОНЛАЙН-ЛОТТЕРЕЯХ
- **$30** у.е. УКРАЛИ АККАУНТ К ОНЛАЙН-КОШЕЛЬКУ С ЭЛЕКТРОННЫМИ ДЕНЬГАМИ
- **$50** ПОКУПКА ЛЖЕ-АНТИВИРУСА, КОТОРЫЙ «СВЕТИТ, НО НЕ ГРЕЕТ»

$226 НА ТЕБЕ ЗАРАБАТЫВАЮТ

- **$25** ПОХИЩЕНИЕ ОТСКАНИРОВАННОГО ИЗОБРАЖЕНИЯ ПАСПОРТА
- **$20** ПОЛУЧЕН ДОСТУП К ПОЧТОВОМУ ЯЩИКУ
- **$3** ЗАРАЖЕНИЕ СИСТЕМЫ ТРОЯНЦЕМ, ВКЛЮЧАЮЩИМ ПК В БОТ-СЕТЬ
- **$10** у.е. ДОСТУП К АККАУНТУ ХОСТИНГ-СЕРВИСА ТИПА RAPIDSHARE
- **$10** ПОХИЩЕНИЕ ДАННЫХ КРЕДИТНОЙ КАРТЫ
- **$150** у.е. КРАЖА «ПРОКАЧАННОГО» ПЕРСОНАЖА ИЗ ОНЛАЙН-ИГРЫ
- **$5** ПАРОЛЬ И ЛОГИН К ОДНОЙ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ
- **$3** у.е. ПАРОЛЬ ОТ IM-МЕССЕНДЖЕРА (ICQ, QIP, PIDGIN И Т.Д.)

Данные «Лаборатории Касперского»

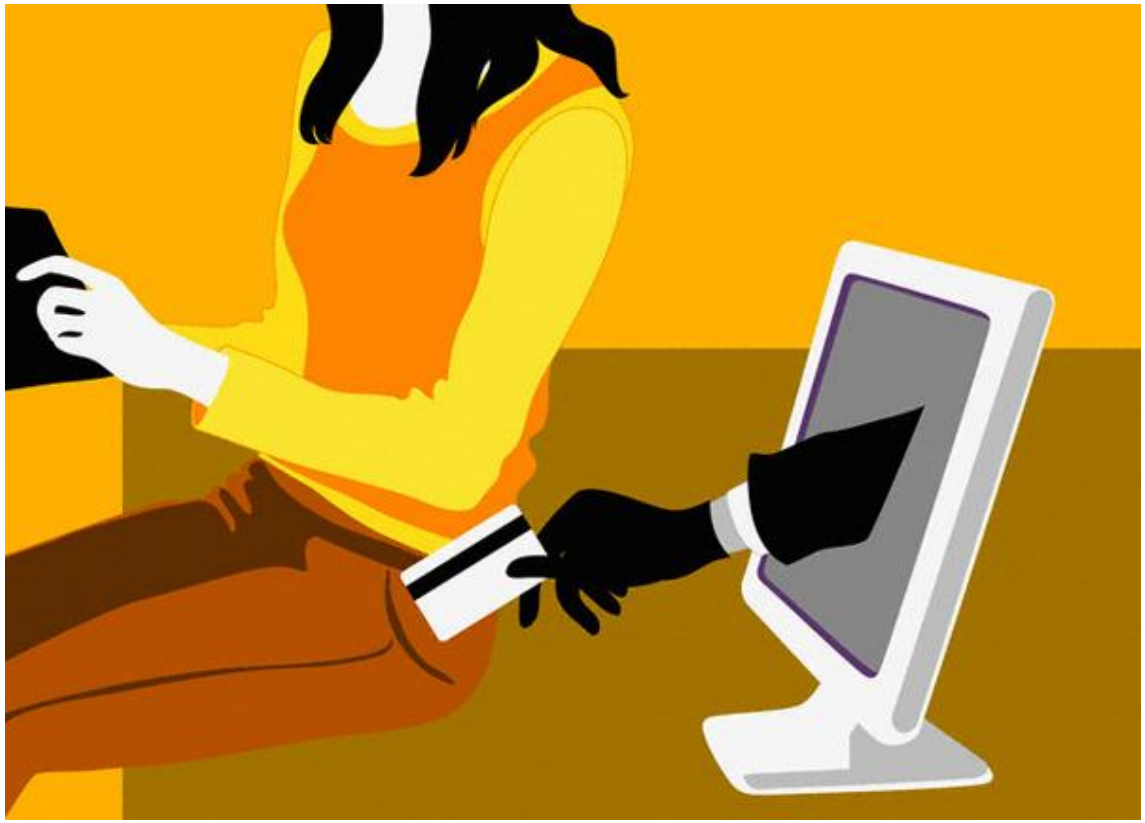
РАЗРАБОТКА КАТЕГОРИЙ КИБЕРПРЕСТУПЛЕНИЙ.

- *Есть несколько путей подразделения киберпреступлений на категории. Мы можем начать с подразделения их на: 1) насильственные или иные потенциально опасные; и 2) ненасильственные преступления.*
- ***Насильственные или иные потенциально опасные***
- *Насильственные и иные потенциально опасные преступления имеют наибольшую опасность по очевидным причинам – они представляют собой физическую опасность человеку или группе лиц. Эти преступления включают:*
  - *Кибертерроризм*
  - *Угроза физической расправы*
  - *Киберпреследование*

КИБЕРВОРОВСТВО:

- *Существует много различных типов киберворовства, или способов использования компьютеров и сетей для хищения информации, денег и иных ценностей. Поскольку прибыль является универсальным мотивом а также по той причине, что способность украсть “на расстоянии” уменьшает для вора риск быть обнаруженным или пойманным, хищения – один из самых популярных видов киберпреступлений.*

- *Кибермошенничество – это получение выгоды или ценностей путем обмана. От воровства оно отличается тем, что жертва добровольно и сознательно отдает деньги или имущество преступнику, но при этом жертва никогда бы этого не сделала, если бы преступник не исказил информацию.*



Самые громкие преступления в мире

Сетевой червь «слопал» космическую программу NASA (1989 год).

Безусловно, крупнейшим и самым загадочным Интернет-преступлением до сих пор остается кошмар из далёкого 1989 года, «Вот были хакеры в прошлом веке...», - вздохнёте вы и будете правы. Неизвестные сумели запустить в компьютерную сеть NASA зловещего червя WANK, вызвавшего катастрофический сбой в программе, Ситуация оказалась настолько серьёзной, что запуски нескольких спутников пришлось перенести на некоторое время, Авторы зловещей шутки до сих пор триумфально вспоминают этот день и пьют шампанское - на свободе.

Хакер «переоборудовал» систему NASA под хранилище фильмов (2001 год)

Компьютерная сеть американского NASA почему-то является непреодолимым магнитом для всех, кто считает себя достойным звания «хакер». Вот и 17-летний Грегори Аарон Хёрнс не придумал ничего лучше, как использовать «свободные площади» компьютерной системы космического агентства для хранения… фильмов, скачанных им из Сети. На устранение последствий невинной шалости юного дарования инженерам NASA понадобилось несколько часов. Лишь через 4 года уже 21-летнего Грегори приговорили к шести месяцам лишения свободы и обязали выплатить штраф за причинённый ущерб. Однако, адвокат юноши с решением суда не согласен - по мнению юриста, его подзащитный сильно изменился за прошедшие годы.

Взломщик получил контроль над американским небом (2000 год)

Пожалуй, на месте сотрудников ФБР вы бы тоже сильно расстроились, обнаружив в свободном доступе в Сети совершенно секретные сведения. А если быть точнее - все исходные коды инновационной компьютерной программы OS/COMET, которая была создана специально для тайной системы NAVSTAR GPS. С помощью последней сотрудники космического отделения Военно-воздушных сил США задавали координаты для космических кораблей, стратегических ракет и спутников. Так каково же было их удивление, когда в декабре 2000 года на бесплатном почтовом сервере FreeboxFreebox.Freebox.com злоумышленник под ником Leaf как ни в чём не бывало выложил столь ценную информацию. Стоит упомянуть, что девять лет назад эта программа считалась одной из самых прогрессивных и была установлена лишь на одной из шести американских наземных станций слежения (остальные должны были обновить лишь в течение 2001 года). Попади код в руки террористов - и ничто не помешало бы им, при наличии определённого оборудования, взять под контроль всё воздушное пространство над Америкой. Кстати, мистический преступник всё ещё не пойман.

Хакер искал в **компьютерах NASA сведения о пришельцах (2002 год)**

Не все системные администраторы одинаково равнодушны к суевериям, британский работник из мира высоких технологий Гари Маккиннон взломал злосчастную компьютерную систему NASA в поисках информации об НЛО. Злодей уверяет, что вскрыл архив секретного «Проекта Открытие», где содержатся сотни фотографий странных объектов и тысячи свидетельств очевидцев о контакте с внеземными цивилизациями. Правда, скептики уверены, что хакер просто пытается отвлечь общественность от своего преступления: британец, проникнув в один из военных компьютеров на базе Форт-Майер в штате Вирджиния, стёр из памяти около 1300 пользовательских паролей и удалил ценную секретную информацию. Сейчас 39-летний компьютерщик ждёт экстрадиции в США, где ему грозит 70-летнее заключение и до 2 миллионов долларов штрафа.

«Хороший хакер» взломал медиа-софт от Microsoft (октябрь 2001)

Но не стоит всех кибер-разбойников считать плохими парнями. Не обошлось в Сети и без своего Шервудского леса, в котором просто не могло не оказаться настоящего Робина Гуда. Парень, известный под ником Beale Screamer, совершенно бескорыстно помог тысячам интернетчиков, написав программу FreeMe для обхода предусмотренной в WMA (Windows Media) -файлах защиты от нелегального копирования. Пока Microsoft безуспешно охотится за «пиратом», его дело живёт и процветает.

Кража как флэш-моб (2008 год)

Одной из самых зрелищных киберкраж в духе фильма «11 друзей Оушена» стал синхронный съём 9 миллионов долларов с сотен зарплатных пластиковых карт по всей планете. В течение 30 минут сразу после полуночи 8 ноября минувшего года в 49 мировых финансовых столицах (Москва, Нью-Йорк, Гонконг - всё, как **и** подобает хорошему голливудскому экшену) «затрещали» 139 банкоматов. Всему виной слабая система безопасности банка RBS WorldPay, благодаря которой злоумышленники сумели украсть нужные данные, подделать пластиковые карты и снять всё без остатка в едином порыве.

Тройка, семёрка, скрытая камера: секретная комбинация вовсе не в картах (2004 год)

Чтобы «надуть» казино Ritz, как оказалось, можно не быть гениальным математиком, просчитывающим всё натри хода вперёд. Достаточно лишь иметь друзей-хакеров, которые установят на твой мобильный телефон программу-сканер, определяющую скорость движения рулетки в лондонском фешенебельном игорном доме и после выдающую комбинацию наиболее вероятных выигрышных чисел. Миллион фунтов стерлингов за один вечер - такой оглушительный джек-пот не мог не насторожить сотрудников казино. Мошенники были успешно разоблачены. Но зато какое удовольствие от игры они успели получить - есть о чём вспомнить за решеткой.

Высокие технологии на службе нелегальных мигрантов (2005 год)

Пожалуй, один из самых забавных «проколов» случился с хакерами, которые зарабатывали себе на хлеб относительно честным путём. Совершенно случайно в одном из английских дворов полисмены обнаружили фургон, нашпигованный высокотехнологичным оборудованием и всевозможными техническими «примочками». Благородные служители закона были несказанно рады ещё бы, предотвратили очередную «кражу века» с участием хитрых IT-шников, а, быть может, даже крупный террористический акт.

Но правда жизни оказалась куда прозаичнее. На самом деле компьютерщики в оцепленном фургоне лишь пытались помочь не владеющим языком иммигрантам пройти культурологический тест «Life in the UK» - последний этап на тернистом пути к вожделенному британскому гражданству. Вся сложная аппаратура была предназначена только для обмана государственной комиссии.

Место киберпреступлений в мире

Сегодня в мире киберпреступления занимают 4-е место

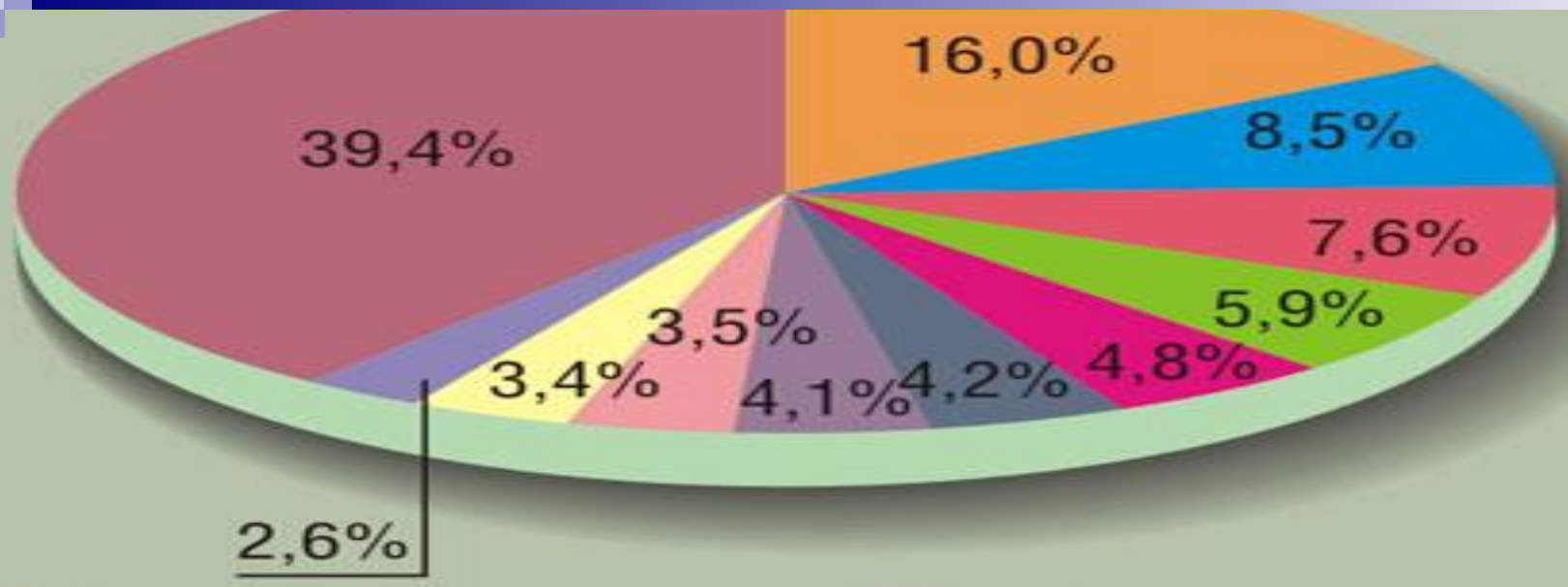
Виртуальные преступления растут с каждым днем. Согласно проведенному преступлению, кибер-преступления занимают четвертое место в мире по частоте совершения.

Вместе с распространением компьютеризации и интернет-технологий экономические преступления, особенно в последние годы, стали новой угрозой.

В наши дни компьютерные технологии и интернет являются неотъемлемой частью деловой и личной жизни человека.

Исследование глобальных экономических преступлений, проведенное с участием деловых кругов в 78 странах, выяснило, что кибер-преступления являются четвертыми в мире по распространению. Привлекается внимание к тому, что каждый пятый из принявших участие в исследовании не обладает знаниями о кибер-безопасности.

В результате исследования также было выяснено, что в мире растет бедность. 34 процента всех опрошенных заявляют, что за последний год они стали жертвами финансовых махинаций. Это означает, что по сравнению с показателями последних 2 лет уровень бедности увеличился на 13 процентов.



Источник: *"Лаборатория Касперского"*.

В Казахстане раскрывают киберпреступления

20 киберпреступлений раскрыты за полгода в Казахстане. Об этом Tengrinews.kz сообщили в Комитете криминальной полиции Министерства внутренних дел республики.
Полицейские отмечают, что участились случаи обнаружения иностранных сайтов террористической направленности.
Генеральная прокуратура Казахстана сообщила о закрытии 15 иностранных сайтов, признанных экстремистскими.

Заключение

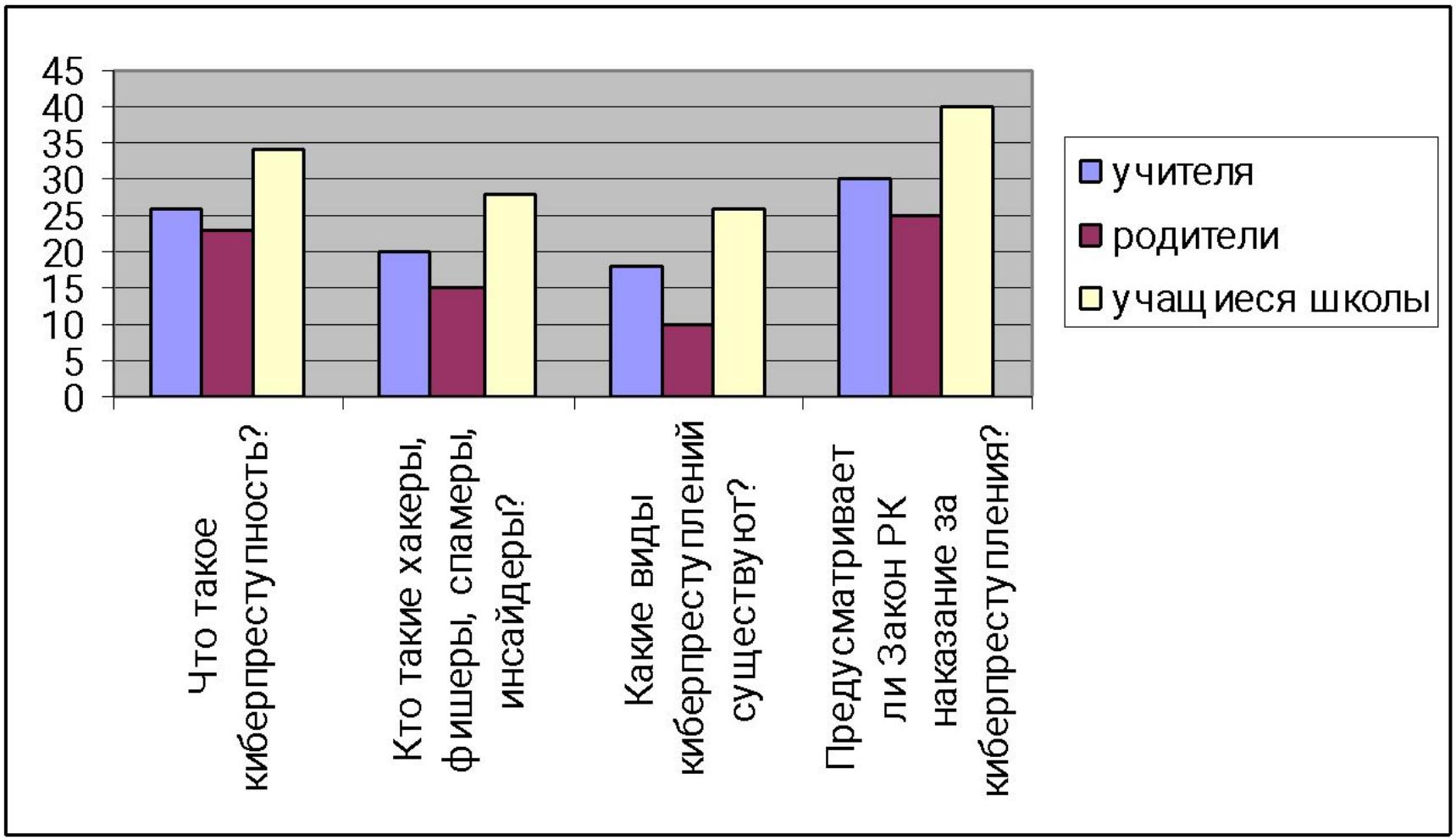
Не секрет, что в настоящее время отмечается серьезный прорыв информационных технологий. Эти разработки существенно облегчили жизнь человеку. С появлением интернета отпала необходимость часами сидеть в библиотеке в поиске нужной информации. Теперь на смену эре механизации пришла компьютерная помощь и автоматизация.
Впрочем, не всегда персональная ЭВМ является для человека другом. Случаются ситуации, когда многочисленные депозитные счета в банках оказываются пустыми вследствие атак хакеров. Кроме того, эти технологичные устройства принесли в наш мир новые болезни в виде электронных вирусов: червей, троянов и т. д. Неужели человечество не сможет противостоять злоумышленникам и вредоносным программам, орудующим в глобальной сети?

В последнее время киберпреступления, в особенности кибертерроризм принимает все более опасный характер, что увеличивает необходимость совершенствования деятельности государственных органов по предотвращению этой опасности. Борьба с незаконными действиями в этой области требует соответствующего технического оборудования, а также специальных знаний и навыков в сфере высоких технологий. В последние годы было уделено большое внимание именно указанным сферам, приняты адекватные меры по усовершенствованию возможностей по борьбе с киберугрозами для нашей страны.

Если люди всех стран будут знать о разных видах киберпреступлений, то тогда будет действовать поговорка «Предупрежден – значит, вооружен» и тогда никто не попадется в лапы мошенников.

Анкета

Вопросы	учителя	родители	учащиеся школы
Что такое киберпреступность?	26	23	34
Кто такие хакеры, фишеры, спамеры, инсайдеры?	20	15	28
Какие виды киберпреступлений существуют?	18	10	26
Предусматривает ли Закон РК наказание за киберпреступления?	30	25	40


45
40
35
30
25
20
15
10
5
0
учителя
родители
учащиеся школы
Что такое киберпреступность?
Кто такие хакеры, фишеры, спамеры, инсайдеры?
Какие виды киберпреступлений существуют?
Предусматривает ли Закон РК наказание за киберпреступления?