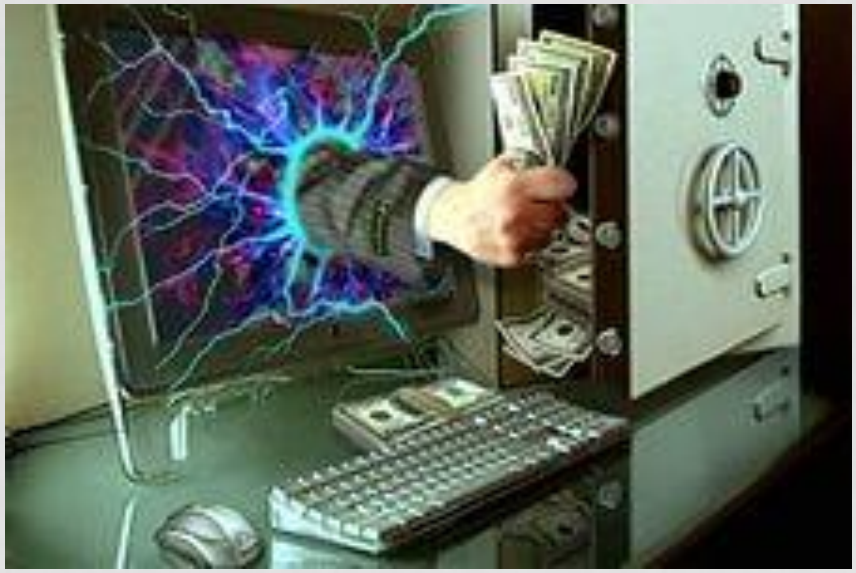
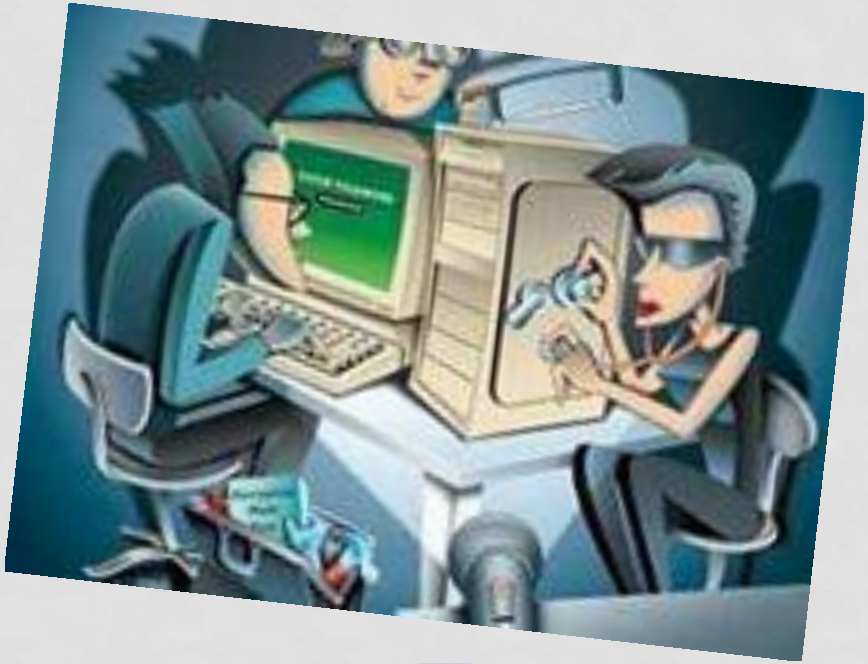
КИБЕРПРЕСТУПНОСТЬ

КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ



К сожалению, развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу персональных компьютеров, информационных систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному антисоциальному явлению, получившим распространенное название – «киберпреступность»



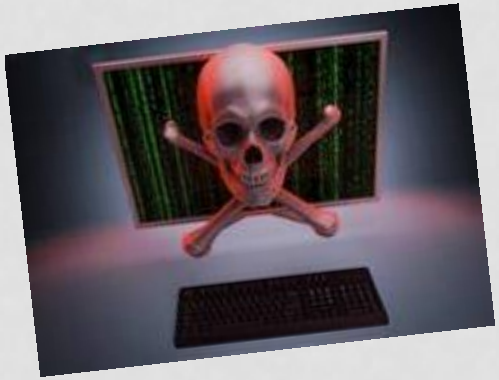
Киберпреступность

— это преступность в так называемом виртуальном пространстве. Виртуальное пространство, или киберпространство можно определить как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

Киберпреступление

— это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства. Человек был уязвим всегда, но недавно мы узнали, что беззащитны вдвойне - не только в реальной жизни, но и в мире, о котором три десятка лет назад не знали ничего - виртуальном мире, киберпространстве, в мире компьютеров. Понятие киберпреступность - это преступные действия, в которых используется глобальная компьютерная сеть Internet. Киберпреступность таит в себе большую общественную опасность. Сегодня значительную долю в общем объеме уголовных преступлений начинает занимать преступность связанная с использованием компьютерных систем и сетей. Ее росту и развитию способствует сама природа данного вида преступления, базирующаяся на открытом и общедоступном характере сети Internet.



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.**

Незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

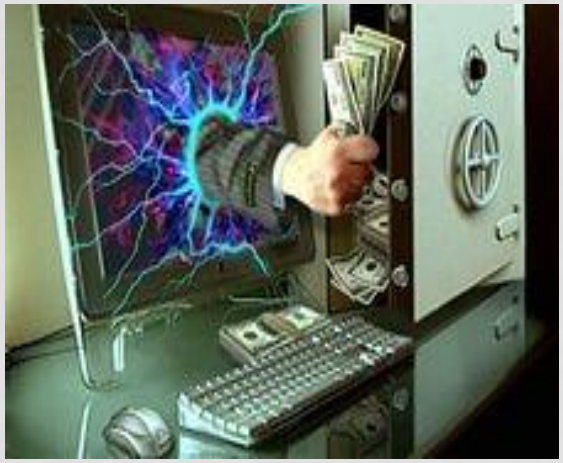
Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

В XXI в. количество атак на информационные системы во всем мире резко возрастает, а их последствия не менее опасны, чем физические нападении на жизненно важные объекты. Такие атаки, произведенные компьютерным путем, могут выводить из строя контрольные системы водо- и энергоснабжения, транспортные узлы и сети, ядерные реакторы, другие стратегические объекты.

Примеры киберпреступлений

«ПЛАСТИКОВЫЕ БАНДИТЫ»

Махинации с пластиковыми картами и электронными платежами – излюбленный вид деятельности сетевых злоумышленников. Преступления в этой сфере условно можно разделить на крупные кражи, осуществляемые организованными преступными группировками, и относительно мелкие акты мошенничества, которые проворачивают воры-одиночки или небольшие шайки.



Сегодня, используя уязвимые места пользовательских компьютеров, злоумышленники могут попытаться совершить целый ряд преступлений: кражу личных данных, зомбирование компьютера с последующим использованием его в бот-сети или нарушение нормального функционирования ПК или информационной сети. Для последнего особенно популярны DDos-атаки, когда группа злоумышленников отправляет на сервер своей жертвы такое число запросов, которое он не сможет обработать.

Мобильное мошенничество :

– Оператор

Пользователю приходит сообщение якобы «от оператора», в котором предлагается позвонить на определенный номер и получить на счет $3 бесплатно. Как правило, деньги действительно поступают, но стоимость звонка при этом выходит в $5-10.

– Дать позвонить

Еще несколько лет назад ситуация, в которой незнакомец просит на улице дать позвонить по мобильному телефону, была чревата возможностью расстаться с аппаратом. Теперь телефоны таким образом не воруют (что не отменяет необходимости быть осторожным). Злоумышленник просто звонит на «нужный» номер, за что и списываются внушительные суммы со счета жертвы.

– Неизвестный номер

Раздается звонок с неизвестного номера и тут же сбрасывается. Афера рассчитана на пагубное любопытство пользователя, который перезванивает по незнакомому номеру и лишается всех средств на счете.

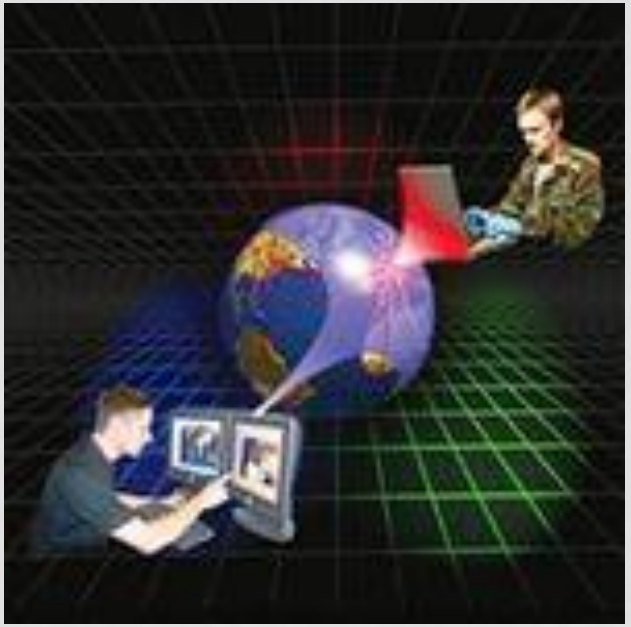
– Донор

Когда с незнакомого номера пишут, что ребенку нужен донор и просят позвонить на определенный номер – это очень циничное мошенничество. Деньги за звонок снимут, но ребенок, скорее всего, так и останется без донора.

– Дешевый контент

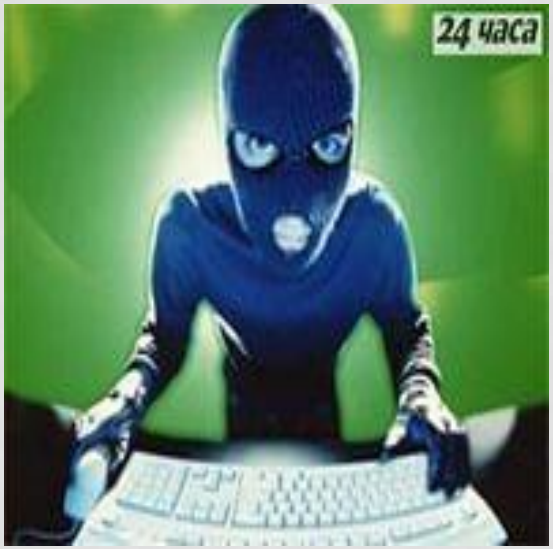
Контент-оператор предлагает за смехотворную плату скачать картинки и мелодии в MP3. Согласившийся пользователь не получает ничего. Либо совсем не то, что заказывал.

Запомните основные правила компьютерной безопасности:



1. Не проходите по присылаемой ссылке от незнакомых людей и не просматривайте прикрепленные файлы
2. Не посещайте вредоносные или незнакомые сайты
3. Делайте резервное копирование своих данных
4. Не используйте в публичных местах Wi-Fi для интернет-платежей
5. Не устанавливайте программы из непроверенных источников
6. Используйте различные сложные пароли и не храните их на компьютере
7. Обновляйте устаревший браузер и свою систему
8. Удалите программное обеспечение, которым вы не пользуетесь
9. В случае потери компьютера, используйте шифрование диска
10. Установите антивирусную программу, регулярно обновляющуюся
11. Не храните на компьютере, имеющем выход в Интернет, никакой личной информации
12. Никогда не подписывайтесь ни на какие компьютерные рассылки.

Вывод



Необходимость защиты от киберпреступников очевидна. Желательно, чтобы на уровне государства решались проблемы борьбы с киберпреступлениями, а повсеместно проводить работу по разъяснению ограждения от киберпреступников. Наша безопасность в наших руках! Мы за безопасность использования информационного пространства.

ИСПОЛЬЗОВАННЫЕ МАТЕРИАЛЫ:

1. HTTP://MVNIK.RU/IMAGES/INFORMATIKA/KIBER.PDF
2. HTTP://WWW.MYSHARED.RU/SLIDE/439133/#
3. HTTP://PPT-ONLINE.ORG/4680
4. HTTP://WWW.KASPERSKY.RU/DOWNLOADS/PDF
5. HTTP://WWW.MYSHARED.RU/SLIDE/439133/#
6. HTTP://WWW.PLUSWORLD.RU/DAILY/KIBERPRESTUPLENIYA-V-ROSSII-VISHLI-NA-INDUSTRIALNIY-UROVEN/

Спасибо за внимание!