ТЕМА: КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

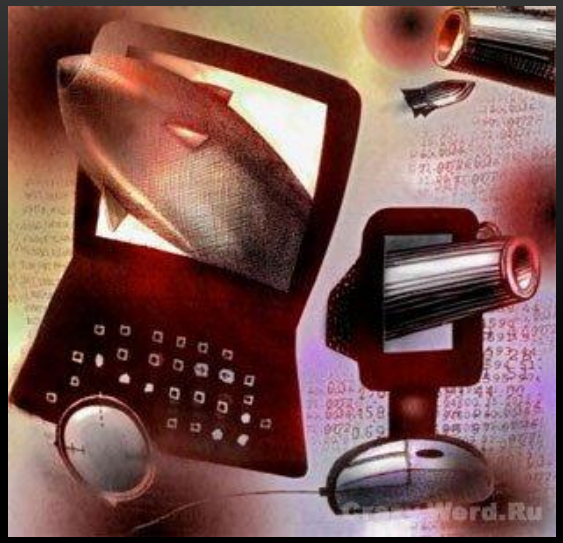
Подготовил студент 229 группы Гаряев Сергей

Научный руководитель Зарипова Р.Ж.

- Объект и предмет исследования – компьютерные преступления, тенденциия и особенности.
- Цели и задачи исследования изучить компьютерные преступления, их криминологически значимые аспекты, необходимые для оценки степени общественной опасности.
- Гипотеза знание сущности и оказываемого вреда компьютерных преступлений, поможет уменьшить ее воздействие.
- Методы исследования: диалектический метод изучения социальных процессов и явлений, сравнительно правовой.
- Экспериментальную базу исследования составляют статистические данные в РФ за 2013 год.

ВВЕДЕНИЕ

Развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу электронно-вычислительных машин, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному социальному явлению, получившим распространенное название – «киберпреступность» и «кибертерроризм».



ПОНЯТИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- Под компьютерными преступлениями чаще всего понимаются преступления, при совершении которых компьютерная техника, информация или электронная обработка информации выступают в качестве предмета или средства совершения преступления. Исходя из такого определения, компьютерным может признаваться любое преступление - хищение, шпионаж, незаконное собирание сведений, которые составляют коммерческую тайну, и т.д., если оно совершается с использованием компьютера.

ОСОБЕННОСТИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

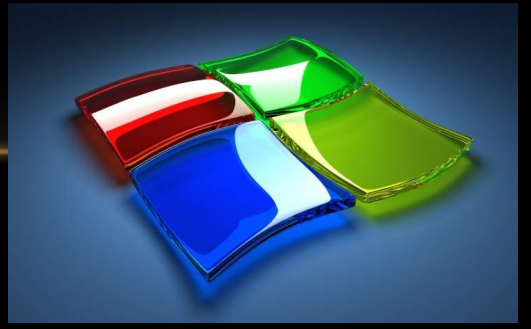
- Важнейшим критерием любого бизнеса является прибыльность, и компьютерные преступления здесь не исключение. Огромные суммы денег оказываются в карманах преступников в результате отдельных крупных афер, не говоря уже о небольших суммах, которые идут просто потоком.
- Минимальный риск и простота исполнения. Вторая причина роста компьютерных преступлений как бизнеса – то, что успех дела не связан с большим риском. В реальном мире психологический аспект преступления предполагает наличие некоторых средств сдерживания. В виртуальном мире преступники не могут видеть своих жертв, будь то отдельные люди или целые организации, которые они выбрали для атаки. Грабить тех , кого ты не видишь, до кого не можешь дотянуться рукой гораздо легче.

ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- Пиратское использование программного обеспечения
- Хакерство
- Программные вирусы
- Компьютерное мошенничество
- Прочие компьютерные преступления

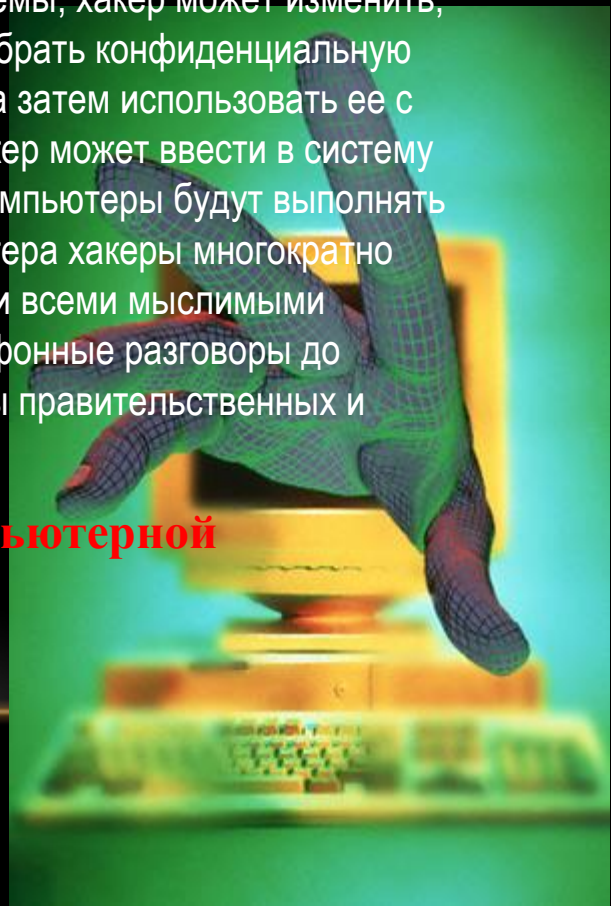
ПИРАТСКОЕ ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

- Компьютерные программы защищены авторским правом, следовательно, их нельзя репродуцировать и использовать без разрешения правообладателя. Пиратские действия в области программного обеспечения - это несанкционированное копирование компьютерных программ для собственного пользования или перепродажи. Часто какая-либо компания или физическое лицо, которые приобрели, например, одну копию той или иной программы, полагают, что это дает им право копировать данную программу. В действительности такое копирование противозаконно до тех пор, пока оно не будет разрешено специальным соглашением (лицензией), оговаривающим условия ее использования. Некоторые люди, стараясь не нарушать законы, все же покупают копию программного обеспечения, а не оригинальную программу у того, кто ее выпускает. Незаконное тиражирование копий программ и продажа фальшивых версий популярного программного обеспечения осуществляется в широких масштабах. Нарушение авторских прав и пиратство в области компьютерного программного обеспечения оказались также в центре международных экономических отношений. Фальшивые программные средства можно приобрести по очень низким ценам на блошиных рынках, в розничной торговле, на восточных базарах и в других слабо контролируемых местах торговли.
- **Статья УК РФ 146 – Нарушение авторских и смежных прав;**



ХАКЕРСТВО

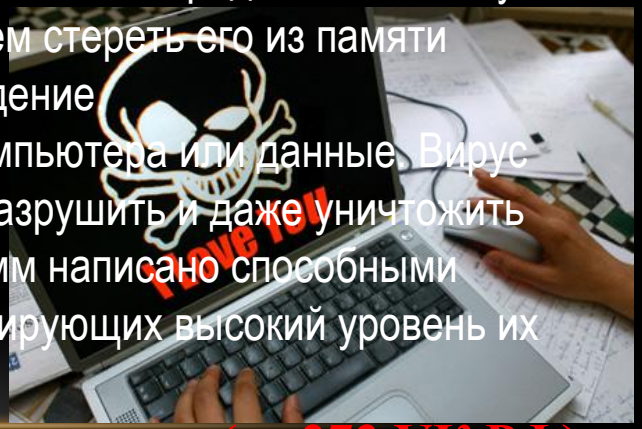
- Один из видов компьютерных преступлений называют "хакерством" (этот термин относится к несанкционированному входу в компьютерную систему). Чтобы получить доступ к "защищенной" компьютерной системе или сети, пользователь должен иметь пароль. Хакеры пользуются множеством разных способов для того, чтобы распознавать секретные пароли или обойти парольную защиту системы. Оказавшись "внутри" компьютерной системы, хакер может изменить, удалить или скопировать данные, хранящиеся в сети. Хакер может собрать конфиденциальную личную и финансовую информацию о компаниях и отдельных лицах, а затем использовать ее с помощью вымогательства или путем банковского мошенничества. Хакер может ввести в систему программные коды или изменить существующие, в результате чего компьютеры будут выполнять команды этого хакера. Со времени появления персонального компьютера хакеры многократно вторгались в компьютерные системы, чтобы манипулировать данными всеми мыслимыми способами - от исправления своих школьных оценок и счетов за телефонные разговоры до "вторжения со взломом" в кажущиеся надежно защищенными системы правительственных и финансовых организаций.
- **Статья 272 УК РФ. Неправомерный доступ к компьютерной информации**



ПРОГРАММНЫЕ ВИРУСЫ

Программный вирус - это компьютерная программа, рассчитанная на то, чтобы нарушить нормальное функционирование компьютера. Вирус можно рассматривать как досадную помеху, на повреждение, которое он способен причинить хранящимся данным, является преступлением.

- программа встраивается в другую внешне вполне безобидную программу и вместе с утилитой запускается на компьютер, он освобождает вирус, который выполняет те неправедные дела, на которые его запрограммировали.
- Некоторые вирусы скорее пустячные или фривольные, нежели зловредные. Они могут воспроизвести на экране эксцентричное сообщение и затем стереть его из памяти компьютера, чтобы нельзя было проследить их происхождение
- Многие вирусы повреждают основные характеристики компьютера или данные. Вирус может также стереть важные компьютерные файлы или разрушить и даже уничтожить данные на жестком диске. Большинство вирусных программ написано способными программистами в качестве эффектных трюков, демонстрирующих высокий уровень их технических знаний.



Разработка и распространение компьютерных вирусов. (ст 273 УК РФ).

КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО

Компьютеры могут быть использованы и в качестве инструментов для совершения различных преступлений, начиная от распространения противозаконных материалов и заканчивая содействием бизнесу, основанному на мошенничестве.

- **Чудо-методики заработка в интернете** - суть данного вида мошенничества в интернете заключается в том, что Вам предлагают купить описание некой секретной методики, как, практически ничего не делая, зарабатывать в Интернете неплохие деньги (обычно фигурируют цифры порядка $50-100 в день). Такую методику заработка в Интернете обычно предлагают купить за $5-10.
- **Программы-генераторы электронных денег** Вам могут предложить купить некую программу, которая собирает бонусы или просто сама каким-то магическим образом генерирует электронные деньги. Очень интересный вид интернет мошенничества с той точки зрения, что народ активно верит в такие «генераторы денег». Стоимость программы обычно около $5
- **Кардинг** вид мошенничества связанный с банковскими картами. Народ активно пытается получить ваши данные по карте и быстренько по ним что-нибудь купить или обналичить. Реализуется самыми разными способами, теми же фишингами, вишингами и т.д., и просто создавая интернет-магазины, которые на самом деле ничего не продают, а просто собирают данные по картам.

КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО

- **СМС-мошенничество** данный вид мошенничества широко распространен как в Интернете, так и в реальном мире. Суть – сделать так, чтобы человек отослал смс на короткий коммерческий номер зачастую за то, что ему абсолютно не нужно. Очень широкая сфера применения и куча способов обмана, достойно серии отдельных статей.
- **Письма счастья** можно сказать, разновидность предыдущего вида мошенничества. Тоже встречается и вне интернета. Письмо сообщает о том, что Вы выиграли в лотерею или что-то в таком духе, но нужно оплатить какой-то налог, чтобы этот выигрыш получить.
- **Фишинг** Данный вид интернет мошенничества заключается в том, чтобы пользователя направить на какой-либо поддельный сайт, который с виду похож на сайт какого-то известного сервиса, платежной системы и т.д. и чтобы человек ввел там свой пароль. Ссылки рассылаются спамерами в основном по e-mail, но используются и другие способы.
- **Статья 159 УК РФ. Мошенничество**

Ты просто не хочешь признаться

ПРОЧИЕ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

- Использование электронных досок объявлений для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности.
- Использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.
- Хищение информации , составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без прав на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества.

ПРИЧИНЫ БУРНОГО РАЗВИТИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- **Такие преступления еще недостаточно широко известны, поскольку они появились в конце 60-х годов, а обратили на себя внимание в начале 90х.**
- **Их сложно выявить, так как современные средства их обнаружения малоэффективны.**
- **Компьютерные преступления сложно предотвратить, поскольку средства и методы защиты постоянно отстают от средств и методов нападения.**
- **Компьютерные преступления совершаются в глобальном масштабе, преступники действуют на большом удалении, проследить их крайне сложно, поскольку они часто прикрываются чужим именем, и след их, если таковой остается, чрезвычайно запутан.**
- **Компьютерная преступность повсеместно принимает организованный характер.**
- **Наказать выявленного преступника не всегда представляется возможным: пользуясь несогласованностью правовых баз различных государств, преступник может совершать "взломы" из страны, где подобная деятельность не является противозаконной.**
- **Нейтрализовать последствия компьютерных преступлений чрезвычайно сложно.**

Борьба с компьютерными преступлениями

- **К техническим мерам** можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое.
- **К организационным мерам** относятся охрана компьютерных систем, возложение ответственности на лиц, которые должны обеспечить безопасность системы.
- **К правовым мерам** следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных. Совсем недавно отечественное законодательство встало на путь борьбы с компьютерной преступностью. И поэтому, представляется весьма важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с компьютерными преступлениями.

Компьютерные преступления в России.

- МВД опубликовало в октябре 2013 года статистику по преступлениям в сфере высоких технологий за первое полугодие 2013 года. По данным Министерства в России было зафиксировано 5696 преступлений, что почти на 11% больше, чем в аналогичном периоде 2012 года. Среди них преобладают преступления, связанные с созданием, распространением и использованием вредоносных программ, а также с мошенничеством в сети Интернет. Интернет-мошенничество, по данным правоохранительных органов, являются самыми распространенными преступлениями в ИТ, и их число продолжает расти. За 6 месяцев 2013 года зафиксировано 1443 таких преступлений (рост на 44%). При этом, по оценкам экспертов, реальное число интернет-мошенничеств в несколько раз выше, так как эти преступления характеризуются высоким уровнем латентности. Особо в МВД отметили увеличение числа преступлений с использованием систем дистанционного банковского обслуживания. В совместную работу по предотвращению преступлений в данной сфере уже включились 23 страны, в числе которых США, Великобритания, Канада, Австралия, Германия, Франция, Бельгия и Нидерланды, говорится в сообщении ведомства. Раньше первое место занимали преступления, связанные с мошенничеством с банковскими картами, но в последний год в лидеры выбились преступления в сфере интернет-банкинга. При этом ущерб от мошенников, взламывающих программы дистанционного банковского обслуживания, доходит до десятков млн. дол.

ОПРОС СРЕДИ УЧАЩИХСЯ

Вид преступления	Всего опрошенных студентов	Количество случаев преступлений
Пиратское использование программного обеспечения	431	143
Хакерство	431	31
Программные вирусы	431	163
Компьютерное мошенничество	431	108
Прочие компьютерные преступления	431	73

Выводы

- Для того чтобы справиться с преступностью в Интернете, необходимо создавать и внедрять защитные стратегии. На самом деле программное обеспечение для борьбы с вредоносными программами и стратегии по управлению рисками важны на всех уровнях и требует совместных усилий. Должен действовать интернет-Интерпол, должна вестись постоянная разъяснительная работа, подобная той, которая ведется по поводу необходимости использовать ремни безопасности в автомобиле.
- Должны существовать правила, соблюдение которых будет обязательно при нахождении в Интернете. Эти же правила должны поддерживать действия правоохранительных органов. Как и в случае с ремнями безопасности, требуется длительная и упорная воспитательная работа для того, чтобы пользователи осознали необходимость таких мер мы можем и должны сделать интернет более безопасным. Для этого нужны более широкомасштабные меры, в них должны принимать участие не одна отдельная компания и не одно отдельное правительство. Нам нужно сообщество единомышленников, каждый из которых внес бы свою лепту в дело информационной безопасности, сообщество, которое может и обязательно добьется успеха.