**Содержание:**

# Введение

Данная Курсовая работа посвящена теме: Анализ совершения Компьютерных преступлений.

В своей работе я хочу раскрыть вопрос о совершении компьютерных преступлений. В данной работе я подробно расскажу о технологиях совершения компьютерных преступлений, о их причинах и методах совершения компьютерных преступлений.

Так же я расскажу о том какую роль играет сеть Internet в сфере компьютерной преступности. В моей курсовой работе будет затронута тема вирусов и защиты от них, но для начала я раскрою смысл определения «компьютерная преступность»

Компьютерная преступность (преступление с использованием компьютера) - представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует.

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел. Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год и составляет около 3.5 миллиардов долларов. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления, составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка - и даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1 процент компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, меньше 10 процентов.

Умышленные компьютерные преступления составляют заметную часть преступлений. Но злоупотреблений компьютерами и ошибок еще больше. Как выразился один эксперт, "мы теряем из-за ошибок больше денег, чем могли бы украсть". Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Основной причиной наличия потерь, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого. Осведомленность конечного пользователя о мерах безопасности обеспечивает четыре уровня защиты компьютерных и информационных ресурсов

# 2. Глава I. Компьютерная преступность в России

В странах, где высок уровень компьютеризации, проблема борьбы с компьютерной преступностью уже довольно давно стала одной из первостепенных. И это не удивительно. Например, в США ущерб от компьютерных преступлений составляет ежегодно около 5 млрд долларов, во Франции эти потери доходят до 1 млрд франков в год, а в Германии при помощи компьютеров преступники каждый год ухитряются похищать около 4 млрд марок. И число подобных преступлений увеличивается ежегодно на 30- 40%.

Поскольку Россия никогда не входила в число государств с высоким уровнем компьютеризации, так как на большей части ее территории отсутствуют разветвленные компьютерные сети и далеко не везде методы компьютерной обработки информации пришли па смену традиционным, то довольно долго российское законодательство демонстрировало чрезмерно терпимое отношение к компьютерным преступлениям. Положительные сдвиги произошли только после ряда уголовных дел, самым громким из которых стало дело одного из программистов Волжского автомобильного завода, умышленно внесшего деструктивные изменения в программу, которая управляла технологическим процессом. что нанесло заводу значительный материальный ущерб. Отечественное законодательство претерпело существенные изменения, в результате которых был выработан ряд законов, устанавливающих нормы использования компьютеров в России.

Главной вехой в цепочке этих изменений стало введение в действие 1 января 1997г. нового Уголовного кодекса. В нем содержится глава "Преступления в сфере компьютерной информации", где перечислены следующие преступления:

неправомерный доступ к компьютерной информации (статья 272):

создание, использование и распространение вредоносных компьютерных программ (статья 273);

нарушение правил эксплуатации компьютеров, компьютерных систем и сетей (статья 274).

Отметим, что уголовная ответственность за перечисленное наступает только в том случае, когда уничтожена, блокирована, модифицирована пли скопирована информация, хранящаяся в электронном виде. Таким образом, простое

несанкционированное проникновение в чужую информационную систему без каких-либо неблагоприятных последствий наказанию не подлежит. Сравните: вторжение в квартиру, дом или офис против воли их владельца однозначно квалифицируется как уголовно наказуемое действие вне зависимости от последствий, в то время как в среде компьютерных преступлений вторжение в частный компьютер не является преступлением.

Следует сказать, что наличие законодательства, регламентирующего ответственность за компьютерные преступления, само по себе не является показателем степени серьезности отношения общества к таким преступлениям. К примеру, в Англии полное отсутствие специальных законов, карающих именно за компьютерные преступления, на протяжении многих лет отнюдь не мешает английской полиции эффективно расследовать дела такого рода. И действительно, все эти злоупотребления можно успешно квалифицировать по действующему законодательству, исходя из конечного результата преступной деятельности (хищение, вымогательство, мошенничество или хулиганство). Ответственность за них предусмотрена уголовным и гражданским кодексами. Ведь убийство и есть убийство, вне зависимости от того, что именно послужило орудием для него.

По данным Главного информационного центра МВД России в 1997 г. доля компьютерных преступлений составила 0,02% от общего числа преступлений в области кредитно-финансовой сферы. В абсолютных цифрах общее количество компьютерных преступлений в этом году превысило сотню, а суммарный размер ущерба --20 млрд рублей.

Однако к этой статистике следует относиться осторожно. Дело в том, что долгое время в правоохранительных органах не было полной ясности относительно параметров и критериев, по которым следовало фиксировать совершенные компьютерные преступления, а также попытки их совершить. Это происходило из-за того, что не было чётких рамок преступления, и не было достаточной осведомленности в компьютерной сфере. Можно предположить, что данные, учтенные официальной статистикой составляют лишь вершину айсберга, подводная часть которого представляет существенную угрозу обществу. И для этого имеются серьезные основания.

Российским правоохранительным органам становятся известны не более 5-- 10% совершенных компьютерных преступлений. Их раскрываемость тоже не превышает 1--5%. Это связано с тем, что хищение информации долгое время может оставаться незамеченным, поскольку зачастую данные просто копируются, и за это время

преступники успевают скрыться. Так же это происходит из-за недостаточной компьютеризации, и правоохранительные органы зачастую даже не догадываются о возможности осуществления некоторых преступлений. Другой возможной проблемой является борьба за собственную репутацию. Жертвы компьютерной преступности (большинство среди них -- частные предприятия) проявляют нежелание контактировать с правоохранительными органами, опасаясь распространения среди вкладчиков и акционеров сведений о собственной халатности и ненадежной работе своей фирмы, что может инициировать отток финансов и последующее банкротство.

## 2.1. Тенденции

По свидетельству экспертов самым привлекательным сектором российской экономики для преступников является кредитно-финансовая система. Анализ преступных деяний, совершенных в этой сфере с использованием компьютерных технологий, а также неоднократные опросы представителей банковских учреждений позволяют выделить следующие наиболее типичные способы совершения преступлений:

Наиболее распространенными являются компьютерные преступления. совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей. В 2008 г. российскими правоохранительными органами были выявлены 85 подобных преступлений, в ходе расследования которых установлены факты незаконного перевода 9,3 млрд. рублей.

За последнее время не отмечено ни одно компьютерное преступление, которое было совершено одним человеком. Более того, известны случаи, когда преступными группировками нанимались бригады из десятков хакеров, которым предоставлялось отдельное охраняемое помещение, оборудованное по последнему слову техники, для того чтобы они осуществляли хищение крупных денежных средств путем нелегального проникновения в компьютерные сети крупных коммерческих банков. Таким образом, они могли перевести всю вину на хакеров, а сами остаться безнаказанными.

Большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков. Результаты исследований, проведенных с привлечением банковского персонала, показывают,

что доля таких преступлений приближается к 70% от общего количества преступлений в банковской сфере. Например, в 2008 г. работники правоохранительных органов предотвратили хищение на сумму в 5 млрд. рублей из филиала одного крупного коммерческого банка. Преступники оформили проводку фиктивного платежа с помощью удаленного доступа к банковскому компьютеру через модем, введя пароль и идентификационные данные, которые им передали сообщники, работающие в этом филиале банка. Затем похищенные деньги были переведены в соседний банк, где преступники попытались снять их со счета с помощью поддельного платежного поручения.

Много компьютерных преступлений совершается в России с использованием возможностей, которые предоставляет своим пользователям Internet. На данный момент это самая большая среда для совершения компьютерных преступлений, и каждый день она рождает новые вредоносные программы.

## 2.2. Internet как среда и как орудие совершения компьютерных преступлений

Уникальность сети Internet заключается в том, что она не находится во владении какого-то физического лица, частной компании, государственного ведомства или отдельной страны. Поэтому практически во всех ее сегментах отсутствует централизованное регулирование, цензура и другие методы контроля информации. Благодаря этому открываются практически неограниченные возможности доступа к любой информации, которые используются преступниками. Сеть Internet можно рассматривать не только как инструмент совершения компьютерных преступлений, но и как среда для ведения разнообразной преступной деятельности.

При использовании сети Internet в качестве среды для преступной деятельности привлекательной для правонарушителей является сама возможность обмена информацией криминального характера. Применять в своей деятельности коммуникационные системы, обеспечивающие такую же оперативную и надежную связь по всему миру, раньше были в состоянии только спецслужбы сверхдержав -- Америки и России, которые обладали необходимыми космическими технологиями.

Другая особенность сети Internet, которая привлекает преступников, -- возможность осуществлять в глобальных масштабах информационно-

психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов.

Однако наибольший интерес сеть Internet представляет именно как орудие для совершения преступлений (обычно в сфере экономики и финансов). В самом простом варианте эти преступления связаны с нарушением авторских прав. К такого рода преступлениям, в первую очередь, относится незаконное копирование и продажа программ, находящихся на серверах компаний, которые являются владельцами этих программ.

Во вторую группу преступлений можно включить нелегальное получение товаров и услуг, в частности, бесплатное пользование услугами, предоставляемыми за плату различными телефонными компаниями, за счет отличных знаний принципов функционирования и устройства современных автоматических телефонных станций. Другие способы незаконного пользования услугами основываются на модификации сведений о предоставлении этих услуг в базах данных компаний, которые их оказывают. Информация о предоставлении какой-то услуги в кредит может либо просто уничтожаться. либо изменяться для того, чтобы потребителем уже оплаченной кем-то услуги стал член преступного сообщества.

Наряду с нелегальным получением товаров и услуг интерес для преступных группировок представляют такие сферы мошеннической деятельности, как азартные игры (казино, лотереи и тотализаторы), организация финансовых пирамид, фиктивных брачных контор и фирм по оказанию мифических услуг. Во всех случаях оперативность взаимодействия с жертвами мошенничества и анонимность самого мошенника весьма привлекательны при совершении компьютерных преступлений в сети Internet.

Одна из предпосылок повышенного интереса, который преступники проявляют к сети Internet, заключается в том, что с развитием компьютерных сетей информация становится все более ценным товаром. Особенно это касается информации, имеющей отношение к банковской сфере -- данные о вкладах и вкладчиках, финансовом положении банка и клиентов, кредитной и инвестиционной политике банка, а также о направлениях его развития. Поскольку в современных условиях субъекты кредитно-финансовой деятельности не могут существовать без взаимного информационного обмена, а также без общения со своими территориально удаленными филиалами и подразделениями, то часто для этих

целей они используют Internet. А это значит, что у преступников появляется реальный шанс получить доступ к сугубо секретной информации о потенциальных объектах своей преступниц деятельности. Уничтожение такой информации преступниками является разновидностью недобросовестной конкуренции со стороны предприятий. которые находятся под "крышей" этих преступников. Даже одна угроза ее уничтожения может сама по себе послужить эффективным средством воздействия на руководство банка с целью вымогательства или шантажа.

Через Internet преступники стремятся также получить возможность нужным для себя образом модифицировать конфиденциальную служебную информацию, которая используется руководством банка для принятия каких-либо важных решений. Дело в том, что ввиду высокой трудоемкости оценки степени доверия к потенциальному получателю банковского кредита в большинстве банков промышленно-развитых стран эта операция автоматизирована. В секрете держатся не только исходные данные для принятия подобных решений, но и сами алгоритмы их выработки. Нетрудно догадаться, какими могут быть последствия, если такие алгоритмы знают посторонние лица, которые могут оказаться в состоянии модифицировать их так. чтобы они вырабатывали благоприятные для этих лиц решения.

Дополнительная сфера компьютерных преступлений, совершаемых через Internet, появилась с возникновением электронных банковских расчетов. т. е. с введением в обращение так называемой электронной наличности. Есть разные способы ее хищения, но все они основываются на модификации информации, отображающей электронную наличность. Информация о наличности, имеющейся на счетах клиентов, переписывается на счета, которыми безраздельно распоряжаются преступники. Изменения также могут быть внесены в сам алгоритм, определяющий правила функционирования системы обработки информации об электронных банковских расчетах. Например, меняется курс валют, чтобы для клиентов банка валюта пересчитывалась по заниженному курсу, а разница зачислялась на счета преступников и многие другие махинации.

## 2.3. Синдром Робина Гуда

В 2008 г. в Экспертно-криминалистическом центре МВД была проведена классификация компьютерных преступников. Обобщенный портрет отечественного

хакера, созданный на основе этого анализа, выглядит примерно так:

- мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере;
- в прошлом к уголовной ответственности не привлекался;
- яркая мыслящая личность;
- способен принимать ответственные решения;
- хороший, добросовестный работник, по характеру нетерпимый к насмешкам и к потере своего социального статуса среди окружающих его людей;
- любит уединенную работу;
- приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуск и отгулы.

По сведениям того же Экспертно-криминалистического центра МВД, принципиальная схема организации взлома защитных механизмов банковской информационной системы заключается в следующем. Профессиональные компьютерные взломщики обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо в доме. в котором не проживают сотрудники спецслужб или городской телефонной сети. Подкупают сотрудников банка, знакомых с деталями электронных платежей и паролями, и работников телефонной станции, чтобы обезопаситься на случай поступления запроса от службы безопасности банка. Нанимают охрану из бывших сотрудников МВД. Чаше всего взлом банковской компьютерной сети осуществляется рано утром, когда дежурный службы безопасности теряет бдительность, а вызов помощи затруднен.

Компьютерные преступления парадоксальны тем, что в настоящее время трудно найти другой вид преступления, после совершения которого его жертва не выказывает заинтересованности в поимке преступника, а сам преступник, будучи пойман, рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов.

Этот парадокс вполне объясним: жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты банком своей репутации) существенно превосходят уже причиненный ущерб;

Преступник, даже получив максимальный срок тюремного наказания приобретет широкую известность в деловых и криминальных кругах, что в дальнейшем позволит ему с выгодой использовать полученные знания.

Таким образом, для общественного мнения в России характерен "синдром Робина Гуда" - преступники-хакеры представляются некими благородными борцами против банкиров. А поэтому хакерство в России, по-видимому, просто обречено на дальнейшее развитие.

Суммируя информацию о компьютерных взломах, которая время от времени появляется в отечественной прессе, можно привести следующее обобщенное (так сказать, "среднеарифметическое") описание одного такого взлома.

## 2.4. История одного компьютерного взлома

В назначенный день около восьми часов вечера все участники планировавшегося взлома компьютерной защиты одного из банков собрались в довольно просторной московской квартире, которая за 3 месяца до начала операции была снята на подставное имя в неприметном доме на тихой улице. Дом был выбран отнюдь не случайно: они выяснили, что в этом доме не проживают сотрудники правоохранительных органов, спецслужб, налоговой полиции и городских телефонных станций, дипломаты, депутаты, террористы, другие хакеры и резиденты иностранных разведок.

Одновременно со взломщиками на "боевое" дежурство заступили подкупленный служащий местной телефонной станции, который на запрос об определении номера телефона квартиры, откуда осуществлялся взлом, должен был сообщить "липовый" номер телефона, и бывшие служащие правоохранительных органов, которые в случае неудачного взлома пообещал организовать защиту штаб-квартиры взломщиков с целью замести следы преступления.

У подъезда дома стоял ничем не примечательный шестисотый "Мерседес", в котором сидели два представителя заказчика-- крупной московской бандитской группировки. Один банк "кинул" дружественную группировке коммерческую фирму на очень большую сумму. Этот банк было решено наказать, запустив в его компьютерную сеть зловредный вирус, который должен был минимум на сутки вывести из строя все банковские коммуникации, включая электрическую, газовую, водопроводную и канализационную, а также мусоропровод.

Главарь банды взломщиков провел инструктаж о бережном обращении с казенным имуществом, раздал компьютеры, бронежилеты, рации и сообщил позывные.

Временная штаб-квартира взломщиков была оснащена по последнему слову техники. На телефонную линию установлено устройство для противодействия подслушиванию. Окна и двери залиты эпоксидной смолой, чтобы не подглядывали соседи. Вся аппаратура подключена к мощным аккумуляторам, чтобы случайные перебои в электропитании не смогли помешать взлому. А сами компьютеры густо посыпаны средством против тараканов и мышей, чтобы исключить непредвиденные сбои в работе оборудования.

Подготовительный этап операции, основная задача которого состояла в подборе входных паролей, начался в 9 часов вечера и продолжался всю ночь, пока в 6 часов утра в штаб-квартире не раздался телефонный звонок. Звонил подкупленный работник банка, который сообщил пароли для входа в банковскую компьютерную сеть.

Главарь приказал по рации всем участникам операции приготовиться к проведению ее заключительной фазы. "Первый готов, второй готов, третий готов" -- понеслось в ответ. "Поехали!" -- послышалась команда главаря. По этой команде дюжие охранники окружили дом: им было приказано никого не впускать и не выпускать без письменного разрешения с подписью главаря, заверенной нотариусом.

Семь смертоносных программ-вирусоносителей устремились по телефонным линиям в атаку на главный сервер банка. Банковские программы защиты были сначала парализованы, а потом полностью смяты превосходящими силами противника. Вырвавшиеся на оперативный простор вирусы учинили в компьютерной сети банка настоящий дебош.

Получив сигнал о проникновении вирусов, главный сервер компьютерной сети банка отключил все коммуникации. В результате город остался без тепла, воды и электричества.

Пока поднятые по тревоге сотрудники отдела безопасности банка торговались, сколько им заплатят за срочность, а потом вылавливали расплодившиеся вирусы, прошли почти сутки. За это время в московской квартире, в которой осуществлялся взлом, были уничтожены все следы пребывания компьютерных взломщиков.

Прямой ущерб, понесенный банком из-за не прохождения платежей, составил сотни тысяч долларов. А заказчикам взлом компьютерной зашиты банка обошелся всего в 20 тыс. фальшивых долларов.

# 3. Глава II. Методы взлома компьютерных систем

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

- атаки на уровне операционной системы;
- атаки на уровне сетевого программного обеспечения;
- атаки на уровне систем управления базами данных.

## 3.1. Атаки на уровне систем управления базами данных

Защита СУБД является одной из самых простых задач. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру, и операции над элементами СУБД заданы довольно четко. Есть четыре основных действия -- поиск, вставка, удаление и замена элемента. Другие операции являются вспомогательными и применяются достаточно редко. Наличие строгой структуры и четко определенных операций упрощает решение задачи защиты СУБД. В большинстве случаев хакеры предпочитают взламывать защиту компьютерной системы на уровне операционной системы и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или плохо протестированная версия СУБД, содержащая ошибки, или если при определении политики безопасности администратором СУБД были допущены ошибки, то становится вполне вероятным преодоление хакером защиты, реализуемой на уровне СУБД.

Кроме того, имеются два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы. В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую

сторону, а разница суммируется в некоторой другой записи СУБД (как правило, эта запись содержит личный счет хакера в банке, а округляемые числовые поля относятся к счетам других клиентов банка). Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на СУБД -- так хитро сформулировать запрос, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

## 3.2. Атаки на уровне операционной системы

Защищать операционную систему, в отличие от СУБД, гораздо сложнее. Дело в том, что внутренняя структура современных операционных систем чрезвычайно сложна, и поэтому соблюдение адекватной политики безопасности является значительно более трудной задачей. Среди людей несведущих бытует мнение, что самые эффективные атаки на операционные системы могут быть организованы только с помощью сложнейших средств, основанных на самых последних достижениях науки и техники, а хакер должен быть программистом высочайшей квалификации. Это не совсем так.

Никто не спорит с тем, что пользователю следует быть в курсе всех новинок в области компьютерной техники. Да и высокая квалификация -- совсем не лишнее. Однако искусство хакера состоит отнюдь не в том, чтобы взламывать любую самую "крутую" компьютерную защиту. Нужно просто суметь найти слабое место в конкретной системе защиты. При этом простейшие методы взлома оказываются ничуть не хуже самых изощренных, поскольку чем проще алгоритм атаки, тем больше вероятность ее завершения без ошибок и сбоев, особенно если возможности предварительного тестирования этого алгоритма в условиях, приближенных к "боевым", весьма ограничены

Успех реализации того или иного алгоритма хакерской атаки на практике в значительной степени зависит от архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки.

Однако имеются атаки, которым может быть подвергнута практически любая операционная система:

- кража пароля;

- подглядывание за пользователем, когда тот вводит пароль, дающий право на работу с операционной системой (даже если во время ввода пароль не высвечивается на экране дисплея, хакер может легко узнать пароль, просто следя за перемещением пальцев пользователя по клавиатуре);
- получение пароля из файла, в котором этот пароль был сохранен пользователем, не желающим затруднять себя вводом пароля при подключении к сети (как правило, такой пароль хранится в файле в незашифрованном виде);
- поиск пароля, который пользователи, чтобы не забыть, записывают па календарях, в записных книжках или на оборотной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять трудно запоминаемые пароли);
- кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);
- полный перебор всех возможных вариантов пароля;
- подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе -- его имени, фамилии, номера телефона, даты рождения и т. д., с использованием сведений о существовании эквивалентных паролей, при этом из каждого класса опробуется всего один пароль, что может значительно сократить время перебора;
- сканирование жестких дисков компьютера (хакер последовательно пытается обратиться к каждому файлу, хранимому на жестких дисках компьютерной системы; если объем дискового пространства достаточно велик, можно быть вполне уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны хакером; для сокрытия следов хакер может организовать эту атаку под чужим именем: например, под именем пользователя, пароль которого известен хакеру);
- сборка "мусора" (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, хакер может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным другими пользователями: например, просмотрев содержимое их "мусорных" корзин);
- превышение полномочий (используя ошибки в программном обеспечении или в администрировании операционной системы, хакер получает полномочия,

превышающие полномочия, предоставленные ему согласно действующей политике безопасности);
- запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);
- подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;
- модификация кода или данных подсистемы защиты самой операционной системы;
- отказ в обслуживании (целью этой атаки является частичный или полный вывод из строя операционной системы);
- захват ресурсов (хакерская программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);
- бомбардировка запросами (хакерская программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера);
- использование ошибок в программном обеспечении или администрировании.

Если в программном обеспечении компьютерной системы нет ошибок и ее администратор строго соблюдает политику безопасности, рекомендованную разработчиками операционной системы, то атаки всех перечисленных пики, малоэффективны. Дополнительные меры, которые должны быть предприняты для повышения уровня безопасности, в значительной степени зависят от конкретной операционной системы, под управлением которой работаем данная компьютерная система. Тем не менее, приходится признать, что вне зависимости от предпринятых мер полностью устранить угрозу взлома компьютерной системы на уровне операционной системы невозможно. Поэтому политика обеспечения безопасности должна проводиться так, чтобы, даже преодолев защиту, создаваемую средствами операционной системы, хакер не смог нанести серьезного ущерба.

- 1. Атаки на уровне сетевого программного обеспечения

СПО является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаше всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные. Поэтому на уровне СПО возможны следующие хакерские атаки:

· прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а, следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);

· перехват сообщений на маршрутизаторе (если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным для хакера является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);

· создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

· навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера);

· отказ в обслуживании (хакер отправляет в сеть сообщения специальною вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Поскольку хакерские атаки на уровне СПО спровоцированы открытостью сетевых соединений, разумно предположить, что дли отражения этих атак необходимо максимально защитить каналы связи и тем самым затруднить обмен информацией по сети для тех, кто не является легальным пользователем. Ниже перечислены некоторые способы такой защиты:

· максимальное ограничение размеров компьютерной сети (чем больше сеть, тем труднее ее защитить);

· изоляция сети от внешнего мира (по возможности следует ограничивать физический доступ к компьютерной сети извне, чтобы уменьшить вероятность несанкционированного подключения хакера);

· шифрование сетевых сообщений (тем самым можно устранить угрозу перехвата сообщений, правда, за счет снижения производительности СПО и роста накладных расходов);

· электронная цифровая подпись сетевых сообщений (если все сообщения, передаваемые по компьютерной сети, снабжаются электронной цифровой подписью, и при этом неподписанные сообщения игнорируются, то можно забыть про угрозу навязывания сообщений и про большинство угроз, связанных с отказом в обслуживании);

· использование брандмауэров (брандмауэр является вспомогательным средством защиты, применяемым только в том случае, если компьютерную сеть нельзя изолировать от других сетей, поскольку брандмауэр довольно часто не способен отличить потенциально опасное сетевое сообщение от совершенно безвредного, и в результате типичной является ситуация, когда брандмауэр не только не защищает сеть от хакерских атак, но и даже препятствует ее нормальному функционированию).

## 3.4. Пять основных технологий, использовавшихся при совершении компьютерных преступлений

Мошенничества:

- Ввод неавторизованной информации
- Манипуляции разрешенной для ввода информацией
- Манипуляции или неправильное использование файлов с информацией
- Создание неавторизованных файлов с информацией
- Обход внутренних мер защиты

Злоупотребления:

- Кража компьютерного времени, программ, информации и оборудования
- Ввод неавторизованной информации
- Создание неавторизованных файлов с информацией
- Разработка компьютерных программ для неслужебного использования
- Манипулирование или неправильное использование возможностей по проведению работ на компьютерах

С другой стороны стоит рассмотреть основные методы, использовавшиеся для их совершения. Они включают:

1. Надувательство с данными. Наверное, самый распространенный метод при совершении компьютерных преступлений, так как он не требует технических знаний и относительно безопасен. Информация меняется в процессе ее ввода в компьютер или во время вывода. Например, при вводе документы могут быть заменены фальшивыми, вместо рабочих дискет подсунуты чужие, и данные могут быть сфальсифицированы.
2. Сканирование. Другой распространенный метод получения информации, который может привести к преступлению. Служащие, читающие файлы других, могут обнаружить там персональную информацию о своих коллегах. Информация, позволяющая получить доступ к компьютерным файлам или изменить их, может быть найдена после просмотра мусорных корзин. Дискеты, оставленные на столе, могут быть прочитаны, скопированы, и украдены. Очень хитрый сканирующий может даже просматривать остаточную информацию, оставшуюся на компьютере или на носителе информации после выполнения сотрудником задания и удаления своих файлов.
3. Троянский конь. Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам)
4. Люк. Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.
5. Технология салями. Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.
6. Суперотключение. Названа по имени программы, использовавшейся в ряде компьютерных центров, обходившей системные меры защиты и

использовавшейся при аварийных ситуациях. Владение этим "мастер-ключом" дает возможность в любое время получить доступ к компьютеру и информации, находящейся в нем

# Заключение

В завершении курсовой работы можно сказать то, что компьютерные преступления — это постоянно развивающийся вид правонарушений. На данный момент нет чёткой схемы и способов защиты от компьютерных преступников, хакеров, вирусов и прочего. Не смотря на многочисленные обновления антивирусных систем, на внесение поправок в уголовный кодекс, компьютерная преступность является самым доходным, но в то же время самым сложный видом преступности.

На данный момент хакерство и компьютерная преступность в России только развивается и набирает обороты. Этому не мало способствует сеть Internet, с помощью которой можно не только обмениваться информацией, но и находить полезные для злоумышленников программы. К этому следует добавить и то, что большинство компьютерных взломов проходит без непосредственного контакта с компьютером жертвы, и любой компьютер подключенный к сети Интернет находиться под угрозой непосредственного взлома и кражи личной информации.

В связи с появление большого количества вирусов и вредоносных программ, начался рост продаж антивирусной продукции. Это говорит нам о том, что эта сфера стала прибыльной не только для преступников и хакеров, но и для тех, кто борется с этой проблемой.

В заключении скажу, что данная сфера постоянно развивается и с каждым днём появляется всё больше вирусов и вредоносных программ с помощью которых всё большее количество хакеров смогу принести всё больший ущерб государству.

# Список литературы

1. Доктрина информационной безопасности Российской Федерации: от 09.10.2000 № Пр-1895: (утвержден В.В. Путиным). - Электрон. Дан. - Режим доступа: http://www.agentura.ru/library/doctrina/

2. Уголовный Кодекс Российской Федерации: от 13.06.1996 N 63-ФЗ: (прият ГД ФС РФ 24.05.1996). - Электрон. Дан. - № 28. - Ст. 273. - Режим доступа: http://www.consultant.ru/popular/ukrf/ Литература

3. Кловский Д.Д. Теория передачи сигналов. - М.: Связь, 1984.

4. Рябков Б.Я., Фионов А.Н. Эффективный метод адаптивного арифметического кодирования для источников с большими алфавитами // проблемы передачи информации. - 1999. - Т.35.

5. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 2006.

6. Акулов О.А., Медведев Н.В. Информатика базовый курс. М.: Омега-Л, 2005.

7. Успенский В. А. Машина Поста. М.: Наука, 1988. Ресурсы Интернет

8. Wikipedia.ru. [Электронный ресурс]: Свободная энциклопедия. - Электро. дан. - М., Режим доступа: http://ru.wikipedia.org