

УДК: 343. 451 (477)



*Владимир Голубев,
к.ю.н., профессор кафедры уголовного права и правосудия
юридического факультета ЗНУ*

Компьютерная преступность - проблемы и решения

Новые информационные технологии дали не только уникальные возможности для более активного и эффективного развития экономики, политики, государства и общества, но и стимулировали возникновение и развитие негативных процессов. Одним из них является появление компьютерной преступности. Одними из главных исторически предпосылок сказавших существенно влияние на рост компьютерной преступности в странах СНГ можно назвать:

1) распад СССР, приведший к выходу из его состава бывших национальных союзных республик и формированию на их основе суверенных государств;

2) частично впервые национальными государственными аппаратами функций полномочного управления своими обществами и государствами в период их становления;

3) противоречивость и несовершенство национальных законодательств;

4) отсутствие унификации законодательства в области информации, информатизации и защиты информации;

5) социально-экономические проблемы, неспособность государственных институтов удовлетворить жизненно необходимые потребности населения;

6) бесхозяйственность и разбалансированность национальных экономик стран бывшего Советского Союза, особенно в кредитно-финансовой, валютно-денежной и товарно-сырьевой сферах.

Одновременно постоянный рост пользователей персональных компьютеров и сети Интернет в последние годы способствовал возникновению новых негативных явлений. Атаки хакеров на web-ресурсы, распространение компьютерных вирусов, Интернет-мошенничество, СПАМ, распространение детской порнографии, и кибертерроризм.

Отстаиваясь от уголовно-правовой дефиниции компьютерных преступлений под компьютерными преступлениями подразумевается общественно опасное действие или бездействие, которое совершается с использованием электронно-вычислительной техники или информации, и причиняет или может причинить, вред имущественным или общественным интересам государства, а также предприятий, учреждений, организаций независимо от формы собственности, общественных формирований и граждан, прав личности.

Анализ современного развития ситуации с точки зрения будущего, можно достаточно смело прогнозировать рост организованной преступности, связанной с использованием электронных средств, одним из которых является компьютер. Финансовые системы мира, несомненно, во все большей степени будут полагаться на обработку данных с помощью ЭВМ и новых информационных технологий и по мере развития техники все большее число стран будет подключаться к существующим и вновь образуемым электронным компьютерным информационным сетям, на которые в настоящее время опирается вся мировая экономика, что неизбежно приведет к появлению еще большего желания обогащения со стороны преступных групп и сообществ. Эту опасную тенденцию мы и наблюдаем в настоящее время.

По оценкам экспертов правоохранительных органов стран Центральной и Восточной Европы по вопросам борьбы с компьютерной преступностью, прибылью преступников от преступлений в сфере использования электронно-вычислительных машин занимает третье место после доходов наркоторговцев и от продажи оружия, а нанесенный ущерб уже сейчас

оценивается миллиардами долларов. Только в США ежегодно экономические убытки от такого рода преступлений оставляют около \$100 млрд.

Характерной особенностью компьютерных преступлений, отличающих их от всех других уголовно-наказуемых дел, является также то, что они обладают очень высокой патентностью и чрезмерно большим размером наносимого ущерба. Считается, что только 10-15% компьютерных преступлений становятся достоянием полиции, так как организации, пострадавшие вследствие совершения подобных преступлений, весьма неохотно предоставляют информацию о них, поскольку это может привести к потере их репутации или совершенно в отношении их повторных преступлений.

В 2004 году Институт компьютерной безопасности в совместной акции с ФБР США провел исследование, предметом которого было определение размеров ущерба, наносимого компьютерными преступлениями, и уровня осведомленности о подобных преступлениях. Опрос, охватывающий 269 организации, от мелких до крупнейших, еще раз подтвердил предположение, что компьютерные преступления представляют реальную угрозу, усугубляемую тем, что она носит скрытый характер [1].

Как видно, самым "дорогим" видом компьютерных преступлений остаются DoS атаки - \$26,064,050. Второе место занимает кража корпоративной информации (промышленный шпионаж) - \$11,460,000, мошенничество с финансовыми ресурсами занимает 5 место - \$7,670,500, на седьмом месте - несанкционированный доступ - \$4,278,205, проникновение в систему - на 11 месте - \$901,500.

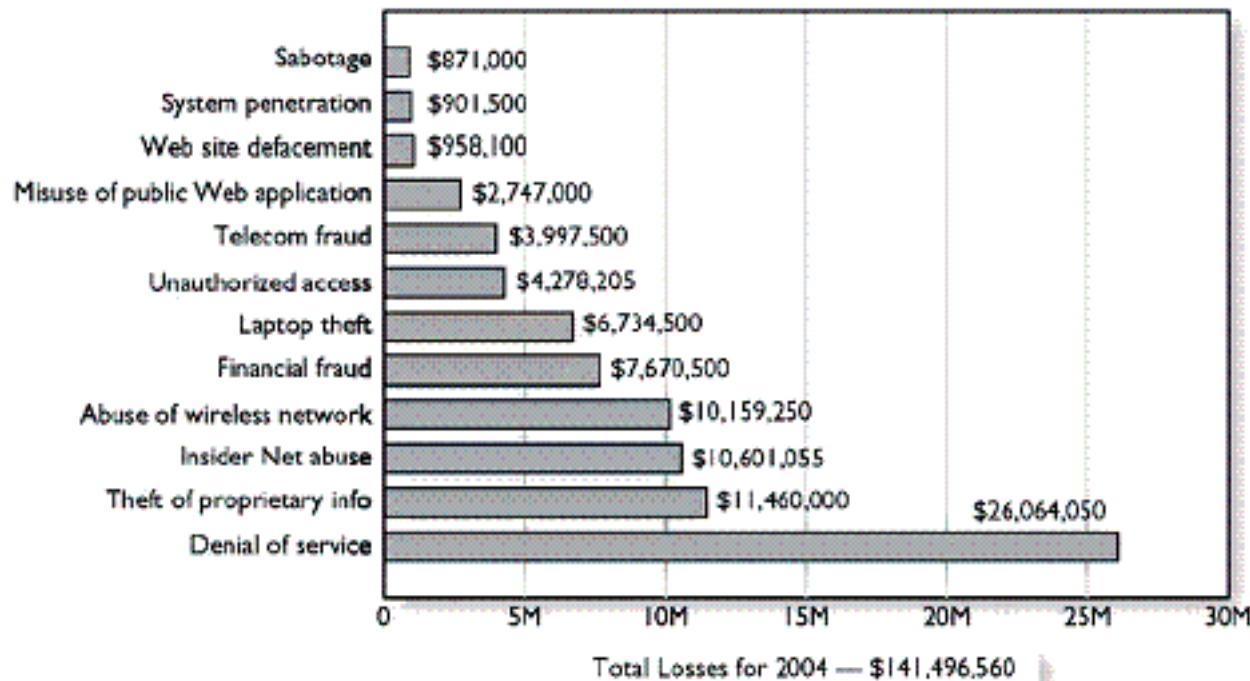
А как обстоят дела с компьютерной преступностью в России? Рост числа правонарушений в сфере компьютерной информации идет не менее быстрыми темпами, чем компьютеризация в России. По данным Главного информационного центра МВД России, в 2004 году зарегистрировано 13723 таких правонарушений, что почти в два раза больше по сравнению с 2003 годом (7053) [2].

Всего 13723 компьютерных преступлений. Из них:

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) - 8002.
2. Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК РФ) - 1079.
3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ) - 11.
4. Нарушение авторских и смежных прав (ст. 146 УК РФ) - 528.

Общий размер причиненного материального ущерба составил 232 млн. 432 тысячи 782 рубля.

Для возмещения ущерба потерпевшим в ходе



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

На рис. 1 видно, что общие потери в 2004 году среди 269 опрошенных респондентов составили \$141,496,560, что меньше чем \$201,797,340 в 2003.

следствия был наложен арест на имущество подозреваемых (обвиняемых) на общую сумму 179 млн. 395 тысяч 592 рубля.

5. Мошенничество (ст. 159 УК РФ) - 371.

6. Причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ) - 2892.

7. Незаконное предпринимательство (ст. 171 УК РФ) - 5.

8. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ) - 480.

9. Изготовление или сбыт поддельных кредитных либо расчетных карт (ст. 187 УК РФ) - 1616. Общий размер причиненного материального ущерба составил 22 млн. 939 тысяч рублей. Для возмещения ущерба потерпевшим в ходе следствия был наложен арест на имущество подозреваемых (обвиняемых) на общую сумму 32 млн. 521 тысяча рублей.

10. Незаконное распространение порнографических материалов или предметов (ст. 242 УК РФ) - 335.

11. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК РФ) - 13.

Впяड़ываясь в скучные цифры статистики, часто возникает вопрос, а почему официальная статистика не всегда соответствует действительности? Официальные лица, в ведении которых находятся государственная статистика о компьютерных преступлениях, считают не всегда возможным представить точные сведения о фактическом состоянии компьютерной преступности. Во-первых, с развитием современных информационных и компьютерных технологий все больше возрастают их функциональные возможности, что, в свою очередь, затрудняет процесс обнаружения факта совершения компьютерного преступления.

В отличие от других традиционных видов преступлений, жертвы компьютерных преступлений зачастую не подозревают, что подверглись преступному посятельству, либо, когда преступление обнаруживается, оно или не передается опласке, или информация о нем в правоохранительные органы поступает слишком поздно, чтобы предпринять необходимые действия для обнаружения виновного лица или лиц.

Во-вторых, лица, производящие дознание и следствие по уголовным делам, связанным с использованием компьютерной техники, часто не обладают достаточным уровнем знаний в области вычислительной техники.

В-третьих, во многих компьютерных системах и сетях отсутствует система защиты, что обуславливает успех посяательства и возможность преступника "уйти незаметно".

В сфере высоких технологий правоохранительные органы еженедельно возбуждают в среднем 170-180 уголовных дел (по информации начальника Бюро специальных технических мероприятий МВД РФ Бориса Мирошникова на международной конференции

"Информационная безопасность региона, организации, граждан" в Москве в июне 2005 г.

По данным за 1 квартал 2005 года сотрудниками Бюро были пресечены и переданы в суд материалы по 2189 преступлениям в сфере высоких технологий. Из них более половины, 1120 дел, были связаны с неправомерным доступом к базам данных в беспроводных и проводных системах. Остальные дела в основном касались нарушения авторских и смежных прав, незаконного оборота радиоэлектронных средств.

Информация о компьютерных преступлениях не всегда становится общезвестна. Пожалуй, никто в мире не имеет сегодня полной картины компьютерной преступности. Понятно, что государственные и коммерческие структуры, которые подверглись нападению, не очень склонны афишировать последствия, причиненные нападением, и "эффективность" своих систем защиты. Поэтому случаи преступлений становятся достоянием гласности далеко не всегда. Но и те факты, которые известны, производят сильное впечатление.

Одним из серьезных причинений раскрываемости такого вида преступлений является транснациональная (трансграничная) составляющая, т.е. когда преступник находится в одном государстве совершает противоправные деяния в отношении объекта, который находится в другом государстве за многие тысячи километров от него.

Тут можно привести классический пример, когда питерский хакер Владимир Левин (Владимир Анатольевич Левин - первый и самый известный российский хакер. Его имя уже стало легендой и включено в список самых выдающихся хакеров мира) используя телекоммуникационные линии связи, несанкционированно входил в систему управления наличными фондами Ситибанка (США) и вводил команды о переводе с различных счетов этого финансового учреждения на свои подставные счета различных сумм денег. В результате Левин в течение нескольких месяцев осуществил не менее сорока переводов на общую сумму свыше \$10 млн. Владимир Левин отсидел 5 лет в американской тюрьме. Однако для российского законодательства Владимир Левин был невзыскан. В то время в России также деяние еще не были уголовно наказуемы.

Нужно отметить, что Российская Федерация стала первой страной в Содружестве Независимых Государств, которая изменила свое уголовное законодательство и впервые в его истории внесла нормы, устанавливающие уголовную ответственность за компьютерные преступления. Глава 28 Уголовного кодекса РФ, принятого 13 июня 1996 года (№ 63-ФЗ) и вступившего в законную силу с 1 января 1997 года, называется "Преступления в сфере компьютерной информации".

Глава 28 УК РФ включает в себя три следующие статьи: 272 "Неправомерный доступ к компьютерной информации", 273 "Создание, использование и распространение вредоносных программ для ЭВМ" и 274 "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети".

Как пример можно привести дело Санкт-Петербургской международной преступной группы, взламывавшей сайты западных букмекерских контор и требовавшей от их владельцев значительные суммы за прекращение атак. Они были задержаны в начале августа 2004 г., подозреваемым удалось получить таким путем сотни тысяч долларов. Параллельно с петербургскими оперативниками ряд задержанной хакеров провели митингеры Саратова и Ставрополя. Предполагаемые преступники, имевшие "коллег" за границей, действовали по одной схеме. Незадолго до начала важных спортивных мероприятий, когда букмекерские конторы принимали ставки на победы и проигрыши наиболее активно, "черные" компьютерщики взламывали серверы. Наибольшие убытки понесли британские компании, их сайты простояли в офф-лайне от нескольких часов до нескольких дней. Потом системные администраторы получали письма с требованием перевести хакерам определенные суммы - до \$40 тыс. в обмен на прекращение атак. Английские букмекеры обратились в Интерпол. Первые 10 злоумышленников были задержаны в Риге. Далее через их показания и с помощью финансовых структур, участвовавших в переводе денег, удалось задержать российских участников группировки. В совместной операции по разработке организованной преступной группы приняли участие правоохранительные органы России, Великобритании, Австралии, США, Канады и Балтийских республик.

28 июля 2004 г. в Москве сотрудниками Управления "К" МВД России была полностью пресечена деятельность крупной организованной преступной группы, которая в течение нескольких лет занималась изготовлением и сбытом специальных технических устройств, предназначенных для негласного получения информации с технических каналов электросвязи, включая компьютерную информацию, циркулирующую в системе ЭВМ.

Еще один пример, когда правоохранительные органы Великобритании выявили сайт в Интернете с рекламой детской порнографии. Было установлено, что провайдер сайта находится в Казахстане. Через Интерпол английские полицейские обратились за помощью в правоохранительные органы Казахстана, которые в свою очередь установили, что данный сайт создан на территории России с компьютера, установленного в одной из квартир Екатеринбурга. Далее было установлено, что снимавшиеся в

фильмах дети - иностранцы, а подозреваемый (житель Екатеринбурга, впоследствии он получил три года условно с испытательным сроком 2 года) только распространял порнопродукцию. В качестве свидетелей были допрошены иностранные граждане, которые на момент расследования уже приобрели и оплатили порнофильмы по \$90 за каждый фильм.

Большое распространение сегодня в Интернете получил DDoS атаки. В рунете даже появилась любопытная "услуга". Киберпреступники предлагают заблокировать доступ пользователей Интернета к "заказанному" сайту всего за \$150 в сутки. Подобные атаки сегодня действительно не редкость, но эксперты подозревают, что за предложением "убить" веб-страницу по предоплате может скрываться обычное мошенничество. "Мы рады вам предоставить качественный сервис по устранению сайтов, мы можем положить любой сайт нашей атакой, которая называется DDoS-атака" - рекламное письмо хакеров. Согласно прайс-листу преступников, шестичасовой простоя веб-сайта обойдется заказчику в \$60, а суточный - в \$150. По предоплате.

В последнее время все чаще слышится слово "Кибертерроризм". Что под этим подразумевается и как проявляется, насколько актуально для стран СНГ?

Анализируя общественную опасность киберпреступности, необходимо отметить проявления высокотехнологического терроризма, особенно компьютерного терроризма или кибертерроризма. Эта форма терроризма вызывает особую озабоченность у экспертов в связи с высокой уязвимостью компьютерных систем управления критической инфраструктурой (транспорт, атомные электростанции, водоснабжение и энергетика), подключенных к Интернету.

Кибертерроризм представляет собой серьезную социально опасную угрозу для человечества, сравнимую с ядерным, бактериологическим и химическим оружием, причем степень этой угрозы в силу своей новизны, не до конца еще осознана и изучена. Опыт, который уже имеется у мирового сообщества в этой области со всей очевидностью свидетельствует о неоспоримой уязвимости любого государства, тем более, что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Обнаружить и нейтрализовать виртуального террориста весьма сложно из-за слишком малого количества оставляемых им следов, в отличие от реального мира, где следов содеянного остается все же больше, особую озабоченность у правоохранительных органов вызывают террористические акты связанные с использованием глобальной сети Интернет.

Явление имеет высокую потенциальную опасность, а в качестве примера можно привести события в январе 2002 года в Украине, когда с целью получения 1 млн.

гривен (\$190 000) невідомі особи повідомили по телефону директору Одеського аеропорту про наявність вибухового пристрою на борту літака, що летить до Вєну, а для підтвердження серйозності своїх намірів і устрашення ними було встановлено вибуховий пристрій напроти входу аерозалю. Злочинники розмістили в мережі Інтернет докладні інструкції про виконання своїх вимог. Головним із них була передача 1 млн грн. Для отримання грошей злочинники планували використати систему Інтернет-платежів "Приват-24", що дозволяє відкрити рахунок управління яким можна виконувати анонімно, знавши тільки логін і пароль. Таким чином, злочинники застали інформаційні технології для забезпечення анонімності і віддаленого повідомлення прогрози і отримання грошей.

Особливо цікаво повідомити про СБУ та управління авіаційної безпеки. Крім виконання типових оперативних заходів, виникла необхідність проведення оперативної установки даних про технічну інформацію в комп'ютерних мережах. Так як на всіх етапах злочинної діяльності був використаний Інтернет, СБУ було прийнято рішення задіявати спеціалістів підрозділу по боротьбі з злочинністю в сфері високіх технологій МВД України, якому поручено встановити осіб, які були відправителями листів з прогрозами і організаторами банківських платежів.

Відповіді провайдерів Інтернет-услугами яких користувалися відправителі листів з прогрозами, показали, в кінцевому підсумку, встановити номери телефонів і адреси, які мають відношення до злочинців, а також про можливість отримати певну доказову інформацію, зберігаються в базах даних Інтернет-провайдера і банку.

Хроніка подій, свідчить про те, що своєчасна і кваліфікована допомога, надана відомством по боротьбі з правопорушеннями в сфері високіх технологій департаменту МВД України співробітникам Департаменту захисту національної державності і боротьбі з тероризмом СБУ, дозволила ізолювати злочинну групу, діяльність якої була своєчасно припинена, а кібертерористи заарештовані за заслугами. В 2001 році хакери-антиглобалісти вломали сервер Всесвітнього Економічного Форуму, неодноразово підвергались нападениям комп'ютерні мережі уряду багатьох держав. За 2001 рік загальне число вторгнень зросло в два рази, порівняно з 2000 роком, і становило 52 тис. При цьому експерти по безпеці передбачають, що за 2002 рік це число зросте ще, як мінімум, в два рази.

Резюмуючи по поводу проблеми кібертероризму, можна сміливо утверждати, що це суспільне небезпечне явище не міф, а реальність, як для всього світового суспільства, так і для нашої держави.

Масовий перехід на методи електронного управління технологічними процесами в виробництві приведе до нашої держави, як уже привело розвинуті держави, до принципово нових видів злочинів, в тому числі до електронного тероризму.

Аналіз світових тенденцій розвитку електронного тероризму, дозволяє зробити висновок, що сьогодні складаються умови для прояву нового виду тероризму - кібертероризму і можна з великою долею ймовірності прогнозувати, що така прогроза з кожним роком буде зростати.

Таким чином, проблема боротьби з комп'ютерною злочинністю сьогодні вже треба поставити на один рівень з тероризмом і організованою злочинністю. При цьому необхідно здійснювати комплексний підхід до рішення цієї проблеми на міжнародному рівні.

Питальною середою для різного роду прояву кіберзлочинності і кібертероризму є хакерство.

Сучасні хакери відрізняються від хакерів 90-х рр. "безобидних шутників і кулішників" (такий вид хакерства відомий в англійському світі як "look-see" хакерство, т. є. хакерство созерцательне или пасивне) все активніше використовують в атаках проти державних комп'ютерних мереж.

Кібератаки і спеціальні знання хакерів широко використовують і використовують на державному рівні, хоча, як і більшість спеціальностей, це все робиться приховано від суспільства.

Настоящий кіберджихад за Кашмир ведуть один проти одного хакери Пакистану і Індії. По повідомленню газети "Хіндустан таймс", пакистанські хакери вламують веб-сайти індійських державних установ. В свою чергу, індійська хакерська група (Indian Snakes), в якості "виртуальної мести" розповсюдила мережу через Yahoo-Q. Головною задачею Yahoo-Q стало виконання DDoS-атак на деякі пакистанські ресурси, серед яких - інтернет-провайдери, сайт фондової біржі в Карачі (Karachi Stock Exchange) і державні ресурси.

В Північній Кореї є колектив "Мирні", військова академія, в якій, як заявляють в Сеулі, готують спеціалістів по веденню електронної війни. Північна Корея має спеціальну військову команду спеціалістів-вломників, яка займається збором секретної інформації про свого сусіда - Республіку Корею. С таким сенсационним утвердженням виступив генерал Сон Юн Кьон, який займається в озброєних силах Республіки Корея питаннями національної безпеки.

По словам генерала Сон Юн Кьона, північнокорейські комп'ютерні вломники вже активно проникають в південнокорейські комп'ютерні мережі.

Особенно хакеров из КНДР привлекают сети государственных ведомств, из которых разведчики пытаются получить секретные сведения. Одновременно КНДР ведет в Интернете и пропагандистскую работу. В начале 2003 года объявил о себе, как о новой террористической организации "Арабский Электронный Джижад" (АЕЛТ), под новым для террористов лозунгом - поставить на колени Интернет Организация АЕЛТ заявила о том, что собирается уничтожить все израильские и американские Web-сайты, а также "все другие неудобные ей сайты".

Все чаще объектами для атак хакеров являются компьютерные сети силовых ведомств (прежде всего Пентагона) и НАСА. Многие случаи становятся достоянием общественности, например в 1990 году группа австралийских хакеров проникла в информационную сеть НАСА, что привело к остановке работы всей системы на 24 часа. Датские хакеры проникли в военные системы США во время телепередачи на США датской телевизионной станции. Они вошли в компьютерные сети Центра космических исследований имени Кеннеди, командования Тихоокеанским флотом США и Ливерморской национальной лаборатории имени Лоуренса.

Исследования, проведенные в 2004 году Центром исследования проблем компьютерной преступности, показали, что именно личностные качества человека и внешняя среда определяют мотивацию принятия решения для преступной деятельности в сфере использования компьютерных технологий. Мотивация включает процесс возникновения, формирования мотива преступного поведения и его цели. Обобщая практику применения законодательства, регулирующего использование электронно-вычислительных машин и систем, можно сделать следующие выводы о субъектах компьютерной преступности [3]:

- компьютерные преступления в 36% совершаются женщинами, в 64% - мужчинами;
- возраст лиц, совершивших эти преступления, колеблется от 16 до 57 лет
- Социальное положение:
 - 6% ученики школ;
 - 6% студенты;
 - 6% сотрудники высших учебных заведений;
 - 18% кассиры банков;
 - 12% программисты и др.

В компьютерную преступность втянут широкий круг лиц, среди которых как высококвалифицированные специалисты, так и дилетанты. Правонарушители имеют разный социальный статус и уровень образования. Их всех можно разделить на две большие группы:

- лица, состоящие с потерпевшим в трудовых или иных деловых отношениях;

- лица, не связанные деловыми отношениями с потерпевшим

К первой группе можно отнести сотрудников, злоупотребляющих своим служебным положением. Это различного рода клерки, работники службы безопасности, контролирующие работники, лица, занимающиеся организационными вопросами, инженерно-технический персонал. По данным нашего исследования доля программистов, инженеров, операторов и других работников организации, совершающих неправомерный доступ к компьютерным системам, составляет 42,3%. Почти вдвое реже такой доступ совершается другими работниками (18,1%), а в 10,7% случаев также правонарушение совершено бывшими работниками организации. Потенциальную угрозу составляют и представители других организаций, занимающиеся сервисным обслуживанием и ремонтом систем.

Ко второй группе относятся лица, имеющие значительные познания в области компьютерных технологий и руководимые в большинстве случаев корыстными мотивами. К этой группе относятся также специалисты-профессионалы, воспринимающие меры по обеспечению безопасности компьютерных систем, как вызов своему профессионализму. Некоторые из них постепенно приобретают вкус к подобной деятельности и решают, что возможно совмещение материальных и интеллектуальных стимулов.

Несмотря на то, что хакерами называют всех виновников компьютерных атак, нами выделены следующие наиболее опасные субъекты неправомерного доступа к компьютерной информации:

- *хакеры-исследователи* - небольшая, но наиболее образованная и талантливая часть сообщества компьютерного андеграунда, основным занятием которых является исследование разнообразного программного обеспечения на уязвимости, которыми может воспользоваться потенциальный взломщик или которые могут улучшить работу компьютерной системы, сети, увеличивая ее эффективность. Также, здесь приводится общее определение термина "хакер" по книге Эрика Реймонда "Новый хакерский словарь" [4];

- *хакеры-взломщики* - довольно многочисленная часть андеграунда, которая в различных целях осуществляет "чистые взломы". Чистые в переводе с компьютерного сленга, это взлом, проникновение, при котором никакая информация не была уничтожена на каком-либо носителе, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения;

- *хакеры-взломцы* - люди, по какому-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам.

Количество разнообразных атак, используемых этим типом людей достаточно велико, но при этом мы вновь не говорим о корыстных целях;

- *хакеры* - люди, которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях;

- *компьютерные хакеры* - люди, но чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи. Необходимо отметить, что почти всегда это не одиночки, а хорошо организованные команды, кланы, со своей четкой специализацией и обязанностями членов такой группы. В числе прочего, в таких группах всегда присутствуют крэмеры, отвечающие за непосредственный взлом компьютерных программ;

- *кибертеррористы* - новая категория компьютерного андеграунда, связанная с феноменом виртуального террора. Одним из первых и самых ярких проявлений этой части был виртуальный террор во время палестинско-израильской интифады в 90-х годах. В данном случае мы имеем дело с людьми, которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб;

- *вирмейкеры* - термин "вирмейкер" ввел в обращение члены известной вирмейкерской группы Stealth. Это люди, которые занимаются написанием компьютерных вирусов. Вирмейкеров еще называют вексерами (от слова Virus exchange) или технокрысами;

- *кардеры* - (от слова card). Одна из наиболее закрытых общностей внутри компьютерного андеграунда в силу своих сложных отношений с законом практически во всех странах мира. Эти люди выбрали своей специализацией изучение особенностей кредитных карт и банкоматов. Наиболее известны кардеры своими незаконными махинациями с кредитными картами и реже - удачными взломами банкоматов. Нанося ежегодный урон банкам и их клиентам, находясь за гранью закона, кардеры образуют собственные сообщества (наиболее известен в России крупный союз кардеров - cardexplant.com) со строгой иерархией и высоким уровнем личной конфиденциальности;

- *фрикеры* - (от слова riveak). Изначально - наука и искусство незаконного подключения к телефонной сети. Уже в конце 80-х, с введением новых, более защищенных стандартов связи, легендарные понятия как "blue box" ушли в прошлое. На данный момент, основной интерес фрикеров во всем мире прикован к спутниковой и сотовой связи. Как и кардеры, это наиболее маргинальные, криминогенные сообщества, деятельность которых незаконна в большинстве стран мира [5, 6].

Выделение типовых моделей разных категорий киберпреступников, знание и учет характерных черт

также субъектов помогает своевременно выявлять и расследовать такие преступления [7].

Если говорить о психическом отношении преступников к совершаемому деянию, то большинство компьютерных преступлений совершаются с прямым умыслом. Разработчики программ и специалисты служб безопасности свели практически к нулю возможность случайного или неосторожного причинения ущерба охраняемым интересам пользователей компьютерной техники.

Для подавляющего большинства компьютерных преступлений характерны корыстные мотивы. Роль преступлений, совершаемых из озорства, незначительна. Встречаются также и политические мотивы, так как глобальные компьютерные системы являются эффективным инструментом политических акций.

Статистическое соотношение различного рода мотивов при совершении компьютерных преступлений по оценке экспертной комиссии Интерпола, таково:

- корыстные мотивы - 66%;
- политические мотивы (терроризм, политические акции) - 17%;
- из исследовательского интереса - 7%;
- из хулиганских побуждений и озорства - 5%;
- из мести - 4%.

С точки зрения психофизиологических характеристик - это, как правило, творческая личность, профессионал, способен идти на технический вызов, риск. В настоящее время крупные компании стремятся привлечь наиболее опытных хакеров на работу с целью создания систем защиты информации и компьютерных систем.

С ростом совершенства компьютерной техники возрастает изоциренность компьютерной преступности. А с развитием глобальной информационной сети Интернет мир столкнулся с таким явлением как "киберпреступность".

Анализ отечественной и зарубежной практики и изучение литературных источников показывают, что возраст компьютерных правонарушителей колеблется в пределах от 14 до 45 лет.

Из материалов экспертных исследований можно сделать вывод, что возраст злоумышленников на момент совершения преступления не превышал 20 лет; 54% - от 20 до 40 лет, 13% - были старше 40 лет. То есть, исследования опровергают сложившийся штамп о том, что хакеры - это, в основном, подростки от 13 до 20 лет.

Преступления в сфере использования компьютерных технологий в 5 раз чаще совершаются мужчинами. Большинство субъектов таких преступлений имеют высшее или несомненное высшее техническое образование (53,7%), а также другое высшее либо несомненное высшее образование (19,2%) [7]. Но в последнее время постоянно увеличивается и доля

женщины в их числе. Это связано с профессиональной ориентацией некоторых специальностей и должностей, оборудованных автоматизированными компьютерными рабочими местами, которые чаще занимают женщины (секретарь, бухгалтер, экономист, менеджер, кассир, контролер и т.д.).

Криминологические исследования свидетельствуют, что:

- 52% установленных правонарушителей имели специальную подготовку в области автоматизированной компьютерной обработки информации,
- 97% были сотрудниками государственных учреждений и организаций, которые использовали компьютерные системы и информационные технологии в своей повседневной деятельности,
- 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

Знание личностных свойств субъектов преступной деятельности в сфере использования компьютерных технологий позволит не только своевременно выявлять, раскрывать и расследовать такие преступления, но и правильно организовать первую линию обороны и тактику противодействия киберпреступности и кибертерроризма.

А кто сегодня ловит хакеров в России?

В 1997 году, в связи с введением в действие Уголовного кодекса РФ и установления уголовной ответственности за преступления в сфере компьютерной информации (глава 28), а также иные виды компьютерных преступлений, Управление "Р" был придан статус оперативно-розыскного подразделения. 7 октября 1998 года Управление "Р" было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ) [8]. На уровне областных Управлений органов внутренних дел Российской Федерации до 1999 года были созданы аналогичные структурные подразделения - отделы БПСВТ. В 2002 году Управление БПСВТ было упразднено, а его штаты, структура и материально-техническое обеспечение были переданы Управлению специальных технических мероприятий (УСТМ) МВД России.

Сегодня эти подразделения называются Отделы "К" (по борьбе с компьютерными преступлениями) при Управлении специальных технических мероприятий МВД России.

Принятое четыре года назад в Минске (Республика Беларусь) Соглашение о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации, заложило хорошую основу стратегии и тактики правоохранительных органов, а также реальный механизм сотрудничества в борьбе с компьютерными преступлениями. Однако до полной реализации принятых совместных обязательств, созданием специальных информационных систем и взаимодействия, к сожалению еще дело не дошло. Украина, как и большинство стран, найдет сегодня на сложном и ответственном этапе решения тех многочисленных проблемы, которые возникают в сфере борьбы с компьютерной преступностью.

1. 2004 CSU/FBI Computer Crime and Security Survey Continue but Financial Losses are Down // http://fi.cmpnet.com/gocs/db_area/pdf/fbi/FBI2004.pdf
2. Статистика компьютерных преступлений в России совершенных в 2004 году // <http://www.crime-research.ru/news/24.05.2005/2007/>
3. Голубев В.А. Компьютерная преступность: мифология и субъект // <http://www.crime-research.ru/news/2004.10.21/1547/>
4. Эрик С. Реймонд. "Новый словарь хакера" - М., 1996 - С.262.
5. Александр Чернавский Анализ формирования компьютерного андеграунда в контексте современной киберкультуры // Компьютерная преступность и кибертерроризм - Запорожье, №2, 2004. - С. 58-65.
6. Голубев В.А., Головин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий // http://www.crime-research.org/library/New_g.htm
7. Голубев В.А. Хакеры или крахеры, а кто это? // <http://www.crime-research.org/library/hack22.html>
8. Cyberpol.ru - компьютерная преступность и борьба с нею // <http://www.cyberpol.ru/cybercops.shtml>