Характеристика жертв компьютерных

преступлений

Вы можете окружить себя кольцом телохранителей и ездить в бронированном лимузине, – но вас оберет до нитки очкарик, забравшийся в ваш компьютер с другого конца города[[1]](#footnote-1).

1.Еще недавно для российского уголовного законодательства не существовало такого понятия как преступность в сфере компьютерной информации. Хотя попытки нелегального проникновения в вычислительные системы с целью ознакомления с ними, исправления, уничтожения или похищения программ и данных появились около 15 лет назад. Количество их растет по мере роста количества домашних компьютеров. Уже тогда были зафиксированы случаи действительно серьезных нарушений: внедрения в военные системы, нарушений работы спутниковых каналов и т.п. Но можно с уверенностью утверждать, что основная часть таких преступлений либо остается нераскрытой, либо замалчивается фирмой или организацией, павшей их жертвой – из страха нанести ущерб своей репутации.

Правда до 1997 года, компьютерная преступность больше беспокоила наших западных соседей. И вот настал момент, когда российский законодатель понял, что ждать больше нельзя и стал серьезно заниматься проблемами компьютерной преступности.

2. Существенную роль в структуре криминологической характеристики компьютерных преступлений играют также обобщенные сведения о потерпевшей стороне. Информация подобного рода позволяет полнее охарактеризовать личность преступника, мотивы совершения преступления и соответственно помогает точнее очертить круг лиц, среди которых следует искать преступника. Именно изучение особенностей потерпевшей стороны и ее поведения (до, в момент и после совершения преступления) дают возможность глубже разобраться во многих обстоятельствах преступления, особенно указывающих на своеобразие, направленность и мотивы поведения преступника, его общие и индивидуальные свойства[[2]](#footnote-2). Между преступником и потерпевшей стороной чаще всего прослеживается определенная взаимосвязь, в силу чего преступники не случайно избирают их объектом своего преступного посягательства.

Проанализировав данные международного комитета по компьютерной преступности, занимающегося исследованиями компьютерных преступлений, а также правовыми аспектами борьбы с этим видом преступности приходим к выводу, что компьютерные преступления представляют собой серьезную угрозу для любой, располагающей компьютерной техникой организации, при этом наряду с высокой степенью риска ей наносится и значительный материальный ущерб. По существующим подсчетам, вывод из строя компьютерной системы в результате действий компьютерных преступников может привести даже самый крупный банк к полному разорению за четверо суток, а более мелкое учреждение – за сутки[[3]](#footnote-3).

3. На данном этапе, опираясь на материалы конкретных уголовных дел отечественной практики потерпевшей стороной или жертвой компьютерных преступлений являются различного рода учреждения, предприятия и организации, имеющие статус юридического лица, поэтому нами используется термин «потерпевшая сторона» и термин «жертва», а не «потерпевший», под которым понимается лицо, которому причинен моральный, физический или имущественный вред[[4]](#footnote-4).

Жертва преступления – понятие более широкое, чем понятие «потерпевший от преступления». Другими словами, жертва – это понятие виктимологическое, потерпевший – уголовно-процессуальное (или гражданско-процессуальное, в зависимости от правовых последствий вреда)[[5]](#footnote-5). Жертва преступления - это человек или определенная общность людей в любой форме их интеграции, которым прямо или косвенно причинен вред преступлением.[[6]](#footnote-6)

Как показывает практика, в качестве жертвы компьютерных преступлений обычно выступает юридическое лицо. Это объяснить можно тем, что в настоящее время в России процесс компьютеризации охватил в основном различные учреждения, организации и предприятия всех форм собственности (т.е. юридических лиц), оставив при этом вне сферы своего влияния большинство населения страны (физических лиц) по причине высокой продажной цены средств компьютерной техники на внутреннем рынке, тем более в условиях глобального кризиса российской экономики. Для подавляющего большинства российских граждан персональный компьютер или другие компьютерные технологии сегодня просто недоступны. Думается, что компьютерная техника, а тем более такое необходимое приложение, как сеть Интернет, в быту россиян широкое распространение не получит еще длительное время. В то время как, например, почти треть американских домовладельцев имеют персональные компьютеры и у 11 млн. из них они оборудованы модемами[[7]](#footnote-7), для получения различных информационных услуг:

* Электронной почты;
* Связи с коллегами по работе;
* Осуществления коммерческих сделок;
* Проведения досуга и т.д.[[8]](#footnote-8)

Тем не менее, думается, что набирающий процесс компьютеризации нашего общества приведет в скором времени к появлению в качестве потерпевшей стороны от компьютерного преступления и физических лиц, как видно из опыта зарубежных стран.

4. До недавнего времени выделялось, исходя из прав собственности на компьютерную систему три основные группы потерпевших сторон от компьютерных преступлений:

К собственникам компьютерной системы можно отнести, как юридических, так и физических лиц. Но выше нами уже отмечалось, что на сегодняшний день собственниками компьютерных систем являются любые юридические лица, чья деятельность непосредственно с компьютерными технологиями. Яркими примерами могут служить компании обслуживающие работу телефонной, в том числе и сотовой связи, пейдженговые компании, банковские структуры, любые пользовательские службы в Интернете и т.д. В Советском райсуде г. Н.Новгорода в ноябре проходило слушание по делу Артема Н. Дело, которое вела ФСБ, суд отправил на доследование. Артем Н. Обвинялся в том, что он проник в компьютерную систему компании ПССР с целью подключения к каналам связи данной компании. Он сумел подключить несколько телефонов, которые в последствии продал. Примечателен тот факт, что за работу данных аппаратов приходилось платить настоящим абонентам компании, которые ничего не подозревали. Кроме того, перед хакером капитулировали сети пейдженговых компаний «Радуга-Поиск» и «Вессолинк», что позволило злоумышленнику просматривать частные сообщения, поступавшие на их пейджеры[[9]](#footnote-9).



Соответственно, вторая группа потерпевших это клиенты, пользующиеся их услугами. Приведем пример, как, клиенты могут стать жертвой компьютерных преступников. В конце 1997 года группа хакеров, назвавшая себя «PANTS/HAGIS», взломала Web-сервер YAHOO[[10]](#footnote-10). В результате взлома системы защиты этого сервера, часть его пользователей получила сообщение с призывом освободить отбывающего тюремное заключение Кевина Митника и заявление о заражении вирусами компьютеров всех, кто пользовался службой YAHOO в течение последнего месяца. Представитель фирмы Дайан Хант подтвердила факт взлома службы, но, по ее словам, в течении 10 минут электронные средства защиты сервера выдали сответствующие сообщения, а технические специалисты практически сразу же локализовали проблему и приняли меры к ликвидации последствий вторжения. Инцендент был исчерпан в течении 15 минут, за исключением конечно отправки множества сообщений пользователям, в которых заявлялось, что каждый пользователь данной поисковой службы получил на свой компьютер тщательно замаскированную логическую бомбу, которая должна активизироваться на Рождество 1998 г., неся разрушения всем компьютерным системам планеты[[11]](#footnote-11). По некоторым данным, действиетльно у некоторых пользователей данной службы обнаружилось действие вирусных программ. Из выше приведенного примера видно что жертвами незаконного компьютерного проникновения помимо клиентов оказалась и сама служба YAHOO.

Третья группа потерпевших страдает от «компьютерных пиратов». «Компьютерные пираты» – занимаются кражей лицензированной компьютерной продукции путем копирования, ее тиражированием и перепродажей преимущественно в Азиатских странах. Краденые программы на CD-ROMax в Азии можно приобрести значительно дешевле их лицензированных аналогов. Когда на 644-мегабайтный компакт-диск втиснуто 30 программ, среди которых такие широко используемые, как Adobe Photoshop, Windows 95, 98 и Microsoft Office, его легальная рыночная стоимость может достичь десятков тысяч долларов. Подпольным дельцам не приходится оплачивать расходы по разработке программ или приобретать лицензии, диски можно штамповать по 60 центов за штуку, а продавать потом от 4 до 15 долларов. Последние статистические данные, представленные Ассоциацией издателей программного обеспечения и «Бизнес Софтвер Элайэнс», свидетельствуют, что продажи пиратских программ в Сингапуре составляет примерно 59%, в Малайзии 80%, Таиланде 80%, Филиппины 92%, Китаем 96% и Индонезией от общего числа продаж[[12]](#footnote-12). Ущерб, который наносится жертвам третьей группы просто огромен.

По неофициальным данным продажа пиратской компьютерной продукции в России составляет не менее 95% от общего числа продаж.

Хотелось бы отметить, что потерпевшие первой группы неохотно сообщают (если сообщают вообще) в правоохранительные органы о фактах компьютерных посягательств. А поскольку они составляют большинство, именно этим можно объяснить высокий уровень латентности компьютерных преступлений.

Поведение жертвы практически всегда определяет сложный комплекс сил. Решение, которое принимает жертва компьютерного преступления, определяется определенными факторами.

Часто организации имеют весьма далекое представление о реальной ценности информации, содержащейся в их компьютерных системах.

Нельзя не учитывать, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, возмещаемого в судебном порядке, многие организации предпочитают ограничиваться разрешением конфликта своими силами, которые нередко завершаются принятием мер, которые вряд ли исключат рецидив компьютерных преступлений.

Органы, ведущие расследование обычно рассчитывают на помощь «потерпевшей стороны», необходимо поднимать большое количество документов, что не всегда желательно.

Раскрытие несостоятельности мер по компьютерной безопасности, принимаемых руководством, может вызвать серьезные внутренние осложнения, а так же подрыв собственного авторитета в деловых кругах и как результат этого – потеря значительного числа клиентов. Это обстоятельство особенно характерно, для жертв первой группы.

Сегодня представляется невероятным, что жертва, потерявшая миллионы, может отказаться от расследования компьютерного преступления. Тем не менее, как показывает практика. Такой «эффект умолчания» достаточно широко распространен[[13]](#footnote-13).

Нельзя недооценивать степень общественной опасности компьютерных преступлений. Отказ потерпевших от уголовного преследования, позволяет действительным преступникам уходить от уголовной ответственности, а другим, потенциальным, преступникам переходить от действий теоретического характера к их практическому осуществлению. Этого допустить нельзя.

1. А.Куприянов. Бесшумная кража / «Soldier of fortune», №3. 1995. С. 42. [↑](#footnote-ref-1)
2. См подробнее: Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия // Под ред. акад. Смарогинского - М.: Право и Закон, 1996. [↑](#footnote-ref-2)
3. Некоторые правовые аспекты защиты и использование сведений, накапливаемой в информационных

   системах // Борьба с преступностью за рубежом. М.: ВИНИТИ. 1990. № 7. С. 37. [↑](#footnote-ref-3)
4. Уголовно-процессуальный кодекс…… [↑](#footnote-ref-4)
5. Полубинский В.И. Правовые основы учения о жертве преступления. Горький, Горьковская высшая школа МВД СССР, 1979. С. 50. [↑](#footnote-ref-5)
6. Д.В.Ривман, В.С.Устинов. Виктимология. Учебное пособие. Н.Новгород, НЮИ МВД РФ. 1997. С. 45. [↑](#footnote-ref-6)
7. Модем – функциональное устройство, осуществляющее связь с удаленными компьютерными коммуникациями по компьютерным сетям. [↑](#footnote-ref-7)
8. Стоит ли злоупотреблять разговорами // МН коллекция, 1994. Декабрь. [↑](#footnote-ref-8)
9. «Суд недели» / Биржа №47, 1998, 26 ноября. [↑](#footnote-ref-9)
10. YAHOO – сетевая служба, а точнее популярный интернетовский поисковый механизм. [↑](#footnote-ref-10)
11. Cм. Подробнее: «Новости Интерента» / «КомПик» №12, 1997. стр. 5. Адрес в Интернете: http://www.kompik.nnov.ru [↑](#footnote-ref-11)
12. Огонь по компьютерным пиратам / Ридерз Дайджест, апрель 1998. С. 105-107. [↑](#footnote-ref-12)
13. Ю.М.Батурин. Проблемы компьютерного права // М.: Юрид. лит., 1991. С. 131. [↑](#footnote-ref-13)