**ИНСТИТУТ МЕЖДУНАРОДНОГО ПРАВА И ЭКОНОМИКИ**
**им. А.С. Грибоедова**

**юридический факультет**
**кафедра уголовно-правовых дисциплин**

**КУРСОВАЯ РАБОТА
по криминологии**
«Преступления в сфере компьютерной информации:
Криминологическая характеристика
 личности преступника»

**Выполнил:**

Студент дневного отделения

3 курса 4 группы

Шестопалов Ю.А.

**Научный руководитель:**

Ермаков В.Д.

**МОСКВА, 1998 год**

ОГЛАВЛЕНИЕ

ОГЛАВЛЕНИЕ 2

ВСТУПЛЕНИЕ 3

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА И ФАКТОР, ОПРЕДЕЛЯЮЩИЙ ОСОБЕННОСТИ ЛИЧНОСТИ КОМПЬЮТЕРНОГО ПРЕСТУПНИКА 4

НЕМНОГО О ЛИЧНОСТНЫХ ОСОБЕННОСТЯХ КОМПЬЮТЕРНЫХ ПРЕСТУПНИКОВ … 8

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ПРЕСТУПНИКИ, ИХ СОВЕРШАЮЩИЕ 12

ЗАКЛЮЧЕНИЕ 27

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 28

ВСТУПЛЕНИЕ

В последнее время всё больше внимания в прессе уделяется так называемым «компьютерным преступлениям». Такое внимание не беспочвенно. Дело в том, что сегодня практически ничто не делается без участия компьютеров – коммуникации, торговля, банковские и биржевые операции и многое, многое другое. Все важнейшие функции современного общества так или иначе «завязаны» на компьютерах, компьютерных сетях и компьютерной информации.

Я не случайно особо выделил торговлю и банковские/биржевые операции среди упомянутых мной сфер деятельности человека, где компьютерная информация занимает одно из главных мест. Здесь вращается не просто компьютерная информация, а так называемые «электронные деньги», которые имеют ни чуть не меньшую ценность, чем привычные банкноты и монеты. А там, где деньги, там и люди, которые жаждут любой ценой обрести их в личную собственность, несмотря на то, что не имеют на эти деньги никаких прав. Это преступники. Компьютерные преступники. Особая разновидность «обитателей» преступного мира. Они не оборванцы, крадущие продукты из супермаркетов; они не «братва», «наезжающая» на торговцев в «комках»; их дело нельзя назвать «мокрым», и деньги, которые им достаются, действительно не пахнут. Так кто же они? Вот в этом я и попробую разобраться в своей работе.

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА И ФАКТОР, ОПРЕДЕЛЯЮЩИЙ ОСОБЕННОСТИ ЛИЧНОСТИ КОМПЬЮТЕРНОГО ПРЕСТУПНИКА

Этот заголовок не случаен, ведь действительно, нельзя рассматривать преступника как нечто, обособленное от всего мира, в том числе и от объекта его посягательств, ведь особенности объекта в определённой степени формируют особенности субъекта.

Итак, компьютерная информация. Как часть информации вообще, она имеет следующие основные свойства:

1. общедоступность, при условии отсутствия особых ограничений на доступ;
2. инвизуальность, т.е. отсутствие способа для человека без специальных инструментов в естественном виде наблюдать и анализировать информацию. Любая информация абстрактна вне привязки к носителю и системе визуализации;
3. 100% идентичность копии и оригинала, т.е. одинаковая информационная ценность исходной информации и её копии на любом носителе при одинаковом конечном методе визуализации.

И эти свойства напрямую определяют то, какими качествами должен обладать преступник, посягающий на компьютерную информацию. Рассмотрим их все.

Начнём, пожалуй, со второго свойства – с инвизуальности. Средством визуализации компьютерной информации является собственно компьютер, инструмент не простой в обращении и требующий от человека, работающего с ним, определённых навыков. Соответственно, можно сделать промежуточный вывод о том, что **компьютерный преступник обладает определённой совокупностью знаний и умений по части общения с компьютерами, программным обеспечением, компьютерными системами и сетями.**

Теперь затронем тему общедоступности. Действительно, компьютерная информация, при условии, что индивид овладел основными навыками общения с инструментом визуализации, становится ему доступной. А так как основные навыки в общении с компьютерной техникой может в настоящее время приобрести практически каждый, то компьютерная информация является общедоступной. Но этот тип информации как никакой другой может быть выведен из разряда общедоступных путём обычных, но многократно усиленных вычислительной мощью компьютеров методов парольной зашиты, аутентичной верификации и шифрования (криптографии). При этом доступ к ней лицам, не знающим пароля, шифра или алгоритма защиты, блокируется практически намертво. Но именно «практически», что в русском языке последних лет стало синонимом слова «почти». *Почти* намертво. При наличии у индивида специальных знаний и навыков, представляется возможным преодоление любых защитных преград на пути к получению информации. Отсюда сам собой напрашивается ещё один вывод: **компьютерный преступник обладает не просто знаниями в области компьютерных технологий, он обладает специальными, достаточно глубокими знаниями, позволяющими ему прокладывать себе путь сквозь любые защитные и оградительные механизмы**.Но детально об этом чуть позже.

Последнее названное мной основное свойство компьютерной информации – полная идентичность копии и оригинала – вроде бы никаких прямых выходов на личность преступника не имеет. Но, так как копия имеет в большинстве случаев ценность, эквивалентную ценности оригинала, необходимость в завладении собственно оригиналом отпадает. Достаточно лишь любым способом сделать копию. При этом факт копирования может быть вообще никак не зафиксирован, поэтому и факт посягательства как бы отсутствует. Так и бывает в большинстве реальных случаев посягательства на компьютерную информацию. Следовательно, налицо повышенная безнаказанность подобного рода преступлений и, соответственно, преступников, их совершающих. Поэтому компьютерному преступнику практически не надо в бояться подозрений, неожиданных визитов представителей «органов» и тому подобных неприятностей. **Компьютерный преступник - это человек, профессионально занимающийся своей деятельностью практически без риска быть уличённым в чём-либо незаконном. Он свободен от сонма страхов, которые преследуют воров, убийц и иных «мирских», некомпьютерных криминальных элементов.**

Сложновато… Но это – «технический» портрет компьютерного преступника, отвлечённый от конкретной личности. Он – как вступление. Компьютерная преступность – явление настолько новое в жизни человечества, что говорить что-либо конкретное просто невозможно – не накопилось ещё достаточно информации и практического опыта. Но этот «портрет» вполне может стать ориентиром в борьбе с компьютерной преступностью, он позволяет выделить основные черты, присущие личности компьютерного преступника независимо от того, кто его родители, в какой социальной среде он вырос, сколько ему лет или был ли он ранее судим за иные преступления. И это только начало …

НЕМНОГО О ЛИЧНОСТНЫХ ОСОБЕННОСТЯХ КОМПЬЮТЕРНЫХ ПРЕСТУПНИКОВ …

Общий портрет – это, конечно, хорошо, иногда даже полезно – хоть какая-то информация. Но – он расплывчатый. И в очень широких пределах. Обычно же, требуется нечто более конкретное и не настолько общее. Да, это уже не универсальный портрет, это «репродукция с корректировками», с поправками на время, место и социально-политическую ситуацию. Особенности, так сказать, «национального» компьютерного преступника. Для России эти «корректировки» наиболее актуальны, так уж повелось, что у нас всё нуждается в корректировке соответственно российскому менталитету. И это не просто «рассуждения для заполнения пустого места в курсовой работе» (почему – станет ясно чуть позднее).

Начнём с того, что и у обывателей, и у работников следственных органов давно сложился яркий такой стереотип компьютерного преступника «made in USSR». Это выросший в семье среднестатистического советского инженера юнец лет 18-ти – 20-ти отроду, с тёмными, длинными, чуть косматыми волосами, в очках, молчаливый, замкнутый, рассеянный, с блуждающим взглядом, помешанный на компьютерах, днями и ночами просиживающий за своей «адской машиной», напрочь игнорирующий события в окружающем мире и девочек. Нельзя сказать, что данный стереотип не имеет права на существование и ни в чём с оригиналом не схож. Самое интересное, что, как показывает статистика и независимые исследования, проведённые, как ни странно, российскими специалистами (и не-специалистами), 20 из 100 «обитателей» преступного мира с «компьютерным уклоном» являют собой стопроцентно «чистых» стереотипных компьютерных преступников. Но только 20 из 100. Остальные 80 в это стереотип не вписываются либо вообще (самый интересный и, кстати, опасный случай), либо частично (это, в основном, промежуточная стадия между стереотипом и его крайней противоположностью).

Стереотипы, как известно, не рождаются на пустом месте. И действительно, в России, так уж исторически сложилось, самое большое число инженеров на душу населения. И, также является бесспорным тот факт, что особым достатком семьи инженеров не отличаются (очевидно, вследствие высокой конкуренции …). Но, как показывает статистика, преемственность в семьях инженеров очень высока (по ряду регионов она достигает 60%, то есть 6 детей из 10 в семьях инженеров идут по стопам родителей). Это можно объяснить семейным духом, высоким уровнем технического образования в российских ВУЗах, и, возможно, чем-то ещё, но я предпочитаю несколько иное объяснение – а) чисто человеческая лень и надежда на «предков» со стороны подрастающего поколения (типа «пойду в матВУЗ – папа с мамой в учёбе подсобят…) и б) родительская надежда на то, что титанический труд инженеров наконец-то оценят, пусть и не в них самих, а в детях (она же – надежда на справедливость – историческую, социальную, экономическую – если такая бывает …). При этом, наследственность в этих семьях, не смотря на известную фразу «на детях гениев природа отдыхает», я бы даже сказал усиленная. Не вдаваясь в биологические детали, скажу лишь, что в отличие от детей музыкантов, дети инженеров в 6 (против 3) случаях из 10 добиваются в жизни больших успехов, чем родители, сохраняя профессиональную принадлежность. О чём это говорит? О том, что дети в семьях инженеров имеют сильную предрасположенность к различным техническим увлечениям. И в наибольшей степени это относится к «лицам мужского пола». Так уж повелось, в силу строения мозга этих самых «лиц». А что сейчас самое передовое, самое интересное в мире техники? Правильно, автомобили и компьютеры. В соотношении где-то 40 на 60. К тому же «сила притяжения» технологии очень велика и к «армии молодых технарей» присоединяются и просто заинтересовавшиеся в компьютерах, родившиеся не в семьях инженеров люди. В результате, в силу стратификации уже внутри слоя людей, приобщившихся к компьютерным технологиям, мы получаем около 20% «ботаников», т.е. «законченных» технарей, действительно помешанных на компьютерах и электронике, и ничего, кроме этого, не воспринимающих, 40% - «средний класс» и 20% - «белые воротнички», снимающие сливки со всего компьютерного и электронного бизнеса. Остальные потихоньку «рассеиваются».

И «всплывают» личности стереотипические (те самые «ботаники») и личности неординарные, в стереотип не вписывающиеся («белые воротнички»). С первыми всё вроде бы понятно – их воспитала социальная среда, в некоторой степени стремление к технике в них заложено генетически. А вот вторая группа – воспитанники среды экономико-политической. Они вовремя осознали свои возможности в конкретный момент времени и в потенциале, определили «рыночную» цену своих знаний, сделали из увлечения карьеру. Их знания в большинстве случаев обширнее и систематизированнее, а следственно и ценнее, чем у самых «загруженных ботаников». Они – настоящая сила как в бизнесе, легальном бизнесе, так и в преступном мире.

Следующая глава посвящена как раз вопросу о том, что же такое компьютерные преступления, чего в них «стоит бояться» и кто же они, конкретные компьютерные преступники …

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ПРЕСТУПНИКИ, ИХ СОВЕРШАЮЩИЕ

Итак, мы подошли к самому интересному в данной работе и в теме о компьютерных преступлениях и преступниках. Так сказать, самое «кровавое» место … с жуткими историями о злобных вирусах и коварных хакерах … И, в принципе, всё почти что так и есть. Итак, перейдём от слов к делу.

УК РФ, Глава 28. Преступления в сфере компьютерной информации. Плод длительной и напряжённой мыслительной деятельности российского законодателя. Его главная роль в том, что он впервые на таком высоком законодательном уровне показал общественную опасность некоторых деяний в области компьютерной информации. Он впервые (правда, в очень интересной манере) позволил дать определение понятию **«компьютерный преступник» – человек, совершивший хотя бы одно из перечисленных в кодексе преступлений в сфере компьютерной информации.**

Отсюда можно сделать вывод, что раз закон выделил 3 глобальных вида компьютерных преступлений (именно глобальных, так как есть ещё под-виды), то можно «рассчитывать» как минимум на 3 вида компьютерных преступников. И соответственно, как минимум на 3 различных (в той или иной степени) личностных типажа.

Первым из преступлений в сфере компьютерной информации закон в статье 272 определяет **«неправомерный доступ к компьютерной информации»**. Что же кроется за этой формулировкой? «Неправомерный доступ» означает получение, в обход определённых запретов и ограничений, возможности тем или иным способом овладеть информацией и/или ознакомиться с ней «воочию». Возвращаясь к «техническому портрету» компьютерного преступника, сразу скажу, что так как **данный тип преступлений в сфере компьютерной информации наиболее распространён и имеет множество модификаций и форм**, следственно, и большинство компьютерных преступников совершают преступления, проходящие именно по этой статье. Преступление и преступник, его личностная характеристика, сильно взаимосвязаны. Что же можно сказать в данном случае?

**Во-первых**, получение **неправомерного доступа** к информации, хранящейся в памяти ЭВМ или на магнитном или ином носителе, **подразумевает** определённую, а учитывая последнее развитие компьютерной техники и информационных технологий, и **усиленную подготовку в области компьютерной технологии**. Что даёт нам это знание в смысле общей оценки личности компьютерного преступника? Он технически подготовлен, обладает набором методов, позволяющих ему подбирать «ключи» к практически любым «электронным» замкам. В большинстве случаев, это выпускник (или студент старших курсов) технического ВУЗа, имеющий постоянный доступ к ЭВМ (в основном, дома), вращающийся в определённых кругах (в основном, среди таких же «закрученных» на компьютерных технологиях «личностях»). Общий возрастной предел – 15..45 лет (случаи проявления компьютерных преступников старше 45 лет не зарегистрированы; возможно, это говорит о том, что с возрастом они либо становятся настолько профессиональными, что пресечение их деятельности становится просто невозможным, либо они «остепеняются», либо просто не доживают [!!!???] до такого почтенного возраста).

Компьютерным преступникам этого типа можно дать определённые характеристики, учесть тенденции формирования преступной личности и разделить на следующие подвиды:

а) **Начинающие.** **Возраст** – 15..25 лет. **Пол** – в подавляющем большинстве случаев мужской. **Образование** – среднее, среднее специальное или высшее, в некоторых случаях неоконченное. Все ступени образования так или иначе связаны с технологией, в основном, компьютерной. **Происходят из** семей среднего достатка. К компьютерной технике «приобщились» в большинстве случаев уже с 8-9 класса средней школы. **Имеют** дома 1 или более персональных ЭВМ, в основном, разного класса (системы начального уровня типа ZX Spectrum или MSX-2, системы второго уровня типа Commodore Amiga или IBM PC). Знание компьютерных технологий не ограничивается языками программирования низкого и высокого уровней (Assembler, C++, Java) и включает в себя знание аппаратной части выбранной платформы. Нигде не работают, либо работают так называемыми «системными администраторами» приходящего или постоянного типа в организациях с развитой компьютерной инфраструктурой, но не могущей позволить себе выплачивать по 500 долларов в месяц специалисту-«компьютерщику». **Личности** увлечённые, если не сказать «помешанные» на компьютерных технологиях. Чаще всего, имеют доступ к глобальной сети Интернет или сетям типа FidoNet. Связь с внешним, «некомпьютерным» поддерживают в ограниченном объёме, предпочитая обществу «светскому» общество людей своего круга. Скрывают подлинные имена за так называемыми «никами» (от английского слова “nickname” – кличка, прозвище, вымышленное имя), причём используют «ники» и в открытом общении. При всей высоте образования (или самообразования) технического, образование гуманитарное явно хромает (в текстах переписки «невооружённым глазом» виден «корявый» стиль и масса грамматических ошибок). В разговоре употребляют особый компьютерный жаргон-сленг, смешивают русский и английский языки. **Характеризуются** несобранностью, некоторой небрежностью, практически постоянно читают литературу «по профессии». Практически целые дни проводят дома за компьютером, в основном за программированием, в сети Интернет или в сетях системы FidoNet, либо посещают специализированные компьютерные клубы и, при наличии средств или знакомств, Интернет-кафе. Преступную деятельность начинают достаточно рано и, в основном, неосознанно, т.е. ещё не осознавая, что их действия квалифицируются по соответствующей статье УК. Установка на преступное поведение формируется стихийно, в основном, под влиянием случайной цепи удачных и неудачных «взломов» защитных программ на других компьютерах. Закрепление такой установки происходит под влиянием «авторитетного мнения старших товарищей», высказанное ими после общения с «новичком» в сетевых «кулуарах». **Практически ежедневно совершают деяния**, подпадающие под статьи 272 (п.1) и 273 (п.1), в основном это получение паролей других пользователей сети Интернет для подключения к этой сети за чужой счёт, доступ к информации о кредитных картах в Интернет-магазинах в России и за рубежом (т.к. Интернет, фактически, интернационален). В более крупных компьютерных преступлениях, в основном по статье 272 (п.2), участвуют либо как соисполнители при организации широкомасштабных «хакерских атак» (атак целью взлома, т.е. преодоления защитных механизмов, и получения доступа к защищённой информации) на сайты (крупные Интернет-представительства компаний и частных лиц), либо как исполнители «на заказ» в тех преступлениях, где требуется долговременная «осада» «объекта» при риске быть засечённым защитными программами или спецслужбами. Очень часто их деятельность связана с незаконным тиражированием и распространением программных продуктов зарубежных и российских производителей.

б) **Закрепившиеся. Возраст** – 20..25 лет. **Пол** – в основном, мужской, но наблюдается тенденция к увеличению числа лиц женского пола (на сегодняшний день это около 5%). **Образование** – среднее, среднее специальное, высшее и незаконченное высшее, в основном – техническое. **Происходят** из семей со средним и выше среднего достатком. Также **имеют персональную ЭВМ**, в основном продвинутого типа (последние модели IBM PC). **Знания в области компьютерной технологии** также на уровне аппаратной части и языков программирования, но более систематизированные и «осмысленные». **При совершении преступлений используют** набор заранее подготовленных «инструментов», в основном, готовые решения, разработанные 1-ой группой или другими людьми своей группы, либо являются организаторами хакерских атак с исполнителями из 1-ой группы. Так же нередко **идут на совершение преступлений «контактным» способом**, часто сопряжённым с насильственными действиями (получение доступа к компьютерной информации с того же компьютера, на котором она размещается, при невозможности удалённого доступа). Если попытаться описать **базисный психотип** компьютерного преступника из этой группы, мы получим лицо достаточно уравновешенное, со сформировавшейся системой взглядов и ценностей, но не высоко-амбициозное. В большинстве случаев, лица, принадлежащие к этой группе, обычно **имеют постоянную работу** в качестве технических консультантов и системных администраторов в фирмах, консультантов в компьютерных фирмах (что позволяет им в определённых случаях получать доступ к компьютеру жертвы «не отходя от кассы», оставляя в его программном обеспечении специальные «чёрные ходы» для возможного дальнейшего использования «в личных целях»). **Преступная «карьера»** либо трансформируется из «карьеры» начинающего, либо формируется сразу в устоявшейся форме при резком «погружении» в криминальную среду при содействии и протекции друзей-«профессионалов». **Внешность** никак практически не выделяется и особенностей, таких как в случае с начинающими, не наблюдается. **Основная сфера «деятельности»** – сетевой взлом, отдельные действия в операциях по получению сильно защищённой информации (в том числе и шпионаж). На более «мелкие» дела идут редко. За хорошую работу берут не менее 1000 долларов США.

в) **Профессионалы. Возраст** – 25..45 лет. **Пол** – мужской - 92%, женский – 8%. **Социальное происхождение** – семьи с достатком выше среднего, которые могли позволить приобретение компьютера ещё в то время, когда они были достаточно дорогими (середина 80-ых, начало 90-ых). **Образование** – высшее техническое, возможно более 1-ого высшего образования (техническое + экономическое или/или юридическое). **Знания в области компьютерных технологий** практически исчерпывающие: люди этой группы владеют несколькими языками программирования всех уровней, в совершенстве знают особенности аппаратной части современных компьютерных систем (не только персональных, но и сетевых систем и специализированных вычислительных комплексов), имеют навыки профессиональной работы с несколькими компьютерными платформами (IBM PC, Apple Macintosh, SUN Microsystems), основными операционными системами (UNIX и клоны, LINUX в различных вариантах, MS DOS, Windows 3.X/NT/9X, OS/2, Novell NetWare/IntranetWare, SUN OS) и большинством пакетов прикладного программного обеспечения специализированного назначения (любое офисное, сетевое программное обеспечение, пакеты разработки приложений и др.), прекрасно информированы об основных системах электронных транзакций (сетевые протоколы, протоколы защищённой связи [биржевые, банковские и правительственные каналы], системах сотовой связи, системах и методах стойкой и супер-стойкой криптографии и успешно используют эти знания в «повседневной деятельности». **Их «работа» подпадает под статью 272 (оба пункта) и некоторые дополнительные статьи (в том числе, шпионаж – военный и промышленный).** В числе совершаемых ими преступлений не числятся «работы» на сумму меньше 5..10 тысяч долларов. **Психотип** крайне уравновешенный, стойкий к внешним воздействиям, с устоявшимися взглядами и системой ценностей. Личности крайне амбициозные, но знающие себе цену. **Мотивация преступного поведения** формируется обычно на стадии освоения «просторов киберпространства». Как личности дальновидные, сразу оценивают свои возможности по извлечению прибыли из своей деятельности. Пробуют профессионально программировать, но сразу понимают, что на Руси этим делом много не заработаешь. И переходят в «теневую область». Так и продолжают. Причём довольно успешно. Добиваются очень многого – благополучия, обеспеченности (правда, ценой достаточно сильной нервотрёпки). Войдя «в поток», начинают вращаться в высших кругах общества. Сейчас они нужные люди. **Имеют связи во многих властных структурах** (причём многие «покровители» обязаны им за определённые услуги), которые используют при необходимости для проникновения на закрытые объекты и для получения кодов доступа в сильно защищённые от «взлома» системы. **Работают в основном «для прикрытия»**, обычно начальниками или замами начальников отделов информационных технологий в банках, в иностранных компаниях и государственных учреждениях, основная же деятельность развёртывается в нелегальной и полулегальной сфере. Связь с «соратниками по ремеслу» поддерживают практически постоянную, но в основном на чрезвычайно конфиденциальном и индивидуальном уровне, крайне редко в прямом общении, в основном через сетевую связь, защищённую стойкой криптографией. Постоянно совершенствуют приёмы и инструменты «работы». **Практически недосягаемы для органов правосудия.** Процент лиц женского пола в данной среде на порядок выше, чем для первых двух типов. Видимо, это связанно с тем, что здесь практически отсутствует так называемая «грязная работа», «заработки» высоки и высок риск, а в рисковых ситуациях, при постоянных стрессах, женщины, как известно, чувствуют себя гораздо увереннее, чем мужчины. **В общем, на лицо стопроцентные профессионалы своего дела.**

В качестве **вывода** о преступниках, совершающих подпадающие под 272 статью УК РФ преступления, можно сказать, что **высокая техническая подготовленность** – их основная черта, **высокая латентность преступлений** – основа их мотивации, **внутренняя предрасположенность** – основное условие вступления на преступный путь, и **социально-экономическая** ситуация в стране – основная причина окончательного выбора.

**Но мы рассмотрели лишь статью 272.** Самую первую. Да, этот «кусок пирога» занимает добрых ¾ от всех преступлений в области компьютерной информации, и тем не менее, следующие статьи и преступники, совершающие указанные в них деяния, также представляют достаточный интерес с точки зрения криминолога. Приступим, помолясь …

**Статья 273.** Цитирую: «Создание, использование и распространение вредоносных программ для ЭВМ». Какая первая ассоциация приходит на ум? Да, **вирусы**. Они самые. Ну, раз они первыми «пришли», первыми их и отработаем.

**Здесь уже не будет деления на 3 группы** – новичков, профессионалов и т.п. – здесь всё более или менее ограничено самой сутью компьютерного вируса. Это обыкновенная программа, набор команд, которые выполняются незаметно для пользователя и результатом имеют некие нежелательные для этого самого пользователя последствия, как то: вывод на экран различных мешающих работе сообщений, стирание и/или произвольную(обычно деструктивную) модификацию содержимого памяти и дисковых накопителей и т.д. А так как это программа, написана она, соответственно, на каком-либо языке программирования, а следственно при участии человека. Программиста. Значит **любого, кто владеет языком программирования**. Сразу такой вот «круг подозреваемых», общая черта для преступника … Но тем не менее, ограничить этот «круг» можно, правда не слишком сильно. Конечно, как я уже сказал, написание вирусов, или, по другому, вредоносных программ доступно практически любому, даже начинающему программисту. Но, у программистов со стажем обычно и так гора работы – им незачем отвлекаться на бесполезные (в большинстве случаев) мелочи типа компьютерных вирусов. Значит, этим «грешат», в основном, именно **начинающие программисты**. Да, вирус может быть не просто забавой, но и мощным оружием в руках «компьютерного террориста» (да, да, есть и такие, но о них чуть позже) и я не просто так оговорился, что вирусы бесполезны в большинстве случаев. Но, тем не менее, изготовлением вредоносных программ для ЭВМ занимаются в 90% случаев именно начинающие программисты **для «пробы пера»** (и это действительно, отвлекаясь от моральной стороны дела, неплохая проба пера – в программе-вирусе применяется очень много серьёзных алгоритмов, несколько сложных для реализации в программном коде, в том числе, полиморфность и криптография, применяемые также в защитных системах). Но «проба пера» случай неинтересный по одной простой причине – экстремально высокая латентность. Ну невозможно, просто технически невозможно, в 999 случаях из 1000 отыскать автора. Вирусов «пробно-перового» плана ежедневно «выпускается» в сеть Интернет, которая является первоочередным «рассадником» «заразы» порядка 30 штук. Все от разных авторов. Со всех концов света. И без видимых признаков идентификации «производителя». И к тому же, даже если автор будет найден, суд вряд ли вынесет ему суровый приговор. Во-первых, **это, в большинстве случаев, несовершеннолетний (15-17 лет)**, а во-вторых, ущерб от его деяния, в большинстве случаев, настолько мизерный, что может просто стать основанием для квалификации этих действий как незначительных для признания преступлением.

А вот что касается 10% вирусов, которые не для «пробы пера», это уже действительно в большинстве случаев умышленные действия для причинения вреда. Я уже упоминал о «компьютерном терроризме». Так вот, это – то самый случай. **И преступники здесь особые. Их портретно-личностные характеристики в данном случае наиболее интересны.**

Как показывает статистика, к сожалению, зарубежная, возраст такого преступника – 23 года и выше. В основном, это высококвалифицированный программист. В большинстве случаев, параллельно совершает деяния, которые (в случае засечения преступника соответствующими службами) могли бы быть квалифицированы по 272 статье. Если вернуться к «списочной» классификации по статье 272, он принадлежит ко 2ой или 3ей группе со всеми вытекающими отсюда личностными характеристиками. Человек, получается, опасный сразу по 2-ум направлениям.

Итак, 273-юю статью тоже «прояснили» в отношении преступников. Пришли, опять же, к неутешительному выводу, подтверждаемому мировой статистикой, что характеристика и описание личности преступника и в данном случае настолько общие, что позволяют делать выводы **только** при наличии достаточного объёма дополнительной информации.

На последок, в заключение этой главы, пару слов о **274-ой статье Уголовного Кодекса**, которая, стараниями предусмотрительного законодателя, увеличила количество составов компьютерного преступления ещё на два.В преступлениях, подпадающих под неё, практически никогда не участвуют описанные мной в этой работе лица. Она несколько специфична и отличается абсолютно «непрограммисткими», нетехническими основным и квалифицированным составами. Здесь преступником может быть практически любой человек, работающий с ЭВМ или «приставленный» к ЭВМ или их комплексу следить за выполнением правил технической безопасности. Кроме того, что он либо администрирует компьютерный комплекс, либо является его пользователем, либо просто получил к нему временный доступ в качестве ни того, ни другого, а, скажем, в качестве уборщика, ничего более сказать просто невозможно. Нет практики. И что самое интересное, нет статистики. Даже зарубежной. Да, преступления подобного рода случаются. Но настолько редко, что выводить типичного преступника и рисовать портрет его личности просто бессмысленно. Подождём-с …

ЗАКЛЮЧЕНИЕ

Вот, в принципе, и всё о компьютерных преступниках. Как ясно из характеристик, личности они интересные. Но, к сожалению, даже обладая достаточно полным набором значащих элементов портрета компьютерного преступника, мы лишь на 30-49% приближаемся к конкретному правонарушителю. Самое печальное, что дальнейшее продвижение по процентной шкале практически исключено – любое высокотехнично исполненное преступление (а практически все компьютерные преступления таковыми и являются) нераскрываемо, если преступник не допустил серьёзных ошибок или его не сдали подельщики.

Но криминологическая характеристика даёт нам, по крайней мере, возможность в определённой степени предвидеть, что может «принести» конкретное правонарушение с точки зрения личности преступника и его действий, на что надо обращать внимание в первую очередь, какие меры планировать, какую реакцию преступника ожидать. А это уже не мало.

Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И российские криминологи и криминалисты внесут в это свой вклад. Ели только российские политики не дадут им умереть с голоду …

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ю.М. Батурин «Компьютерная преступность и компьютерная безопасность»
2. Компьютерный еженедельник «Компьютерра»
3. Интернет-ресурсы, IRC-каналы и материалы конференций