УДК 004.056.57

С.В. Ченушкина

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Ченушкина Светлана Владимировна
Svch2003@yandex.ru
ФГАОУ ВПО «Российский университет образовательных информационных технологий», Россия, г. Екатеринбург

COMPUTER CRIMES AND TYPES OF COMPUTER CRIMES

Chenushkina Svetlana Vladimirovna
Russian State Vocational Pedagogical University, Russia, Yekaterinburg

Аннотация. *Статья рассказывает о видах компьютерной преступности, основных действующих лицах и их мотивов, приводятся примеры конкретных преступлений в разных сферах.*

Abstract. *Article tells about types of computer crime, the main characters and their motives, examples of concrete crimes in different spheres are given.*

Ключевые слова: *компьютерная преступность; компьютерные угрозы.*
Keywords: *computer crimes; computer threats.*

Компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. Согласно экспертным оценкам, она способна нанести ущерб, сопоставимый с объемом хищений произведений искусства во всем мире.

По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 млрд долл. Причем многие потери не обнаруживаются или о них не сообщают.

В 2012 г. число зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации составило 10 227 преступлений, что на 28,3 % выше показателя 2011 г. (7 974 эпизода). В 2011 г. число аналогичных посягательств составило - 7 142 преступления, что на 37,2 % меньше, чем в 2010 г. (12 698 эпизода). В 2014 г. МВД зарегистрировало в России 11 000 компьютерных преступлений. Об этом со ссылкой на заявление начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова сообщает ТАСС. По словам Мошкова, на долю краж и мошенничеств в 2014 г. пришелся 41% киберпреступлений (в 2013 г. этот показатель составлял 30%). Опрошенные «Ведомостями» эксперты рассказывают, что вести учет компьютерных преступлений непросто, но общее их число во много раз превышает данные из статистики МВД. Реальное количество киберпреступлений в России минимум в 5 раз больше, подсчитывает гендиректор компании Digital Security (анализ защищенности компьютерных систем) Илья Медведовский. Количество взломов почты, например, исчисляется миллионами, а они тоже являются киберпреступлениями, говорит руководитель департамента расследований инцидентов Group-

IB (расследование киберпреступлений) Дмитрий Волков. Он сообщает, что попытки хищения денег происходят намного реже, чем взломы почты, но не менее 100 000 в год и часть из них блокируется банками. По данным Group-IB, в 2013 г. киберпреступники заработали в России и СНГ $2,5 млрд [1].

Дело в том, что официальная статистика учитывает только поданные заявления от потерпевших, объясняет Волков. Люди крайне редко пишут заявления в случае DDoS-атак, кражи логинов и паролей, а также установки вредоносных программ, продолжает эксперт. Наибольшую опасность представляет компьютерная преступность в финансовой сфере. Отмечается тенденция к росту компьютерных преступлений в банковской сфере. Согласно результатам независимых опросов, проведенных социологической службой "Кассандра", каждый второй респондент спрогнозировал рост банковских убытков из-за возрастания вероятности мошенничества.

Все лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

- лица, не связанные трудовыми отношениями с организацией жертвой, но имеющие некоторые связи с нею;
- сотрудники организации, занимающие ответственные посты;
- сотрудники пользователи ЭВМ, злоупотребляющие своим положением

Среди основных мотивов компьютерных преступлений выделяют обычно два: корыстный и желание продемонстрировать собственный профессионализм - так называемый "интеллектуальный вызов". Комплекс причин и условий компьютерной преступности составляют, по мнению большинства авторов, следующие обстоятельства: высвобождение и сложности трудоустройства высокоинтеллектуальной и профессиональной части населения, связанной с наукой, тонкими технологиями, обороной и т.п.; безработица интеллектуальной элиты общества; возможность быстрого обогащения путем компьютерных хищений с незначительной вероятностью разоблачения ввиду высокой латентности компьютерных преступлений; недостаточная защищенность автоматизированных систем обработки данных; отставание технической оснащенности, профессионализма сотрудников правоохранительных органов от действий профессиональных компьютерных преступников; отсутствие обобщенной следственной и судебной практики расследования компьютерных преступлений; лояльное отношение общества к такого рода преступлениям ввиду использования лицами, их совершающими, интеллектуального способа обогащения и т.п.

Западные специалисты подразделяют представляющий опасность персонал на категории в соответствии со сферами деятельности:

1. Операционные преступления - совершаются операторами ЭВМ, периферийных устройств ввода информации в ЭВМ и обслуживающими линии телекоммуникации.
2. Преступления, основанные на использовании программного обеспечения, обычно совершаются лицами в чьем ведении находятся библиотеки программ; системными программистами; прикладными программистами; хорошо подготовленными пользователями
3. Для аппаратурной части компьютерных систем опасность совершения преступлений представляют: инженеры системщики, инженеры по терминальным устройствам, инженеры-связисты, инженеры-электронщики.

4. Определенную угрозу совершения компьютерных преступлений представляют и сотрудники, занимающиеся организационной работой: управлением компьютерной сетью, руководством операторами; управлением базами данных; руководством работой по программному обеспечению.

5. Определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование ЭВМ.

Особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Например, около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих - системные администраторы и другие сотрудники служб автоматизации банков [2].

«Инцидент, случившийся в 1983 году на ВАЗе, вошел в историю компьютерных преступлений как один из первых фактов внесения вредоносных изменений в существующие программы для ЭВМ. Программист, автор системы, регулирующей подачу деталей на главный конвейер, был недоволен оценкой руководством своей работы. В то же время его коллеги, написавшие свои программы с ошибками, получали крупные премии за их исправление. Отреагировал на это он следующим образом - вписал в свою программу несколько строк, и подача деталей стала периодически разлаживаться. Во время одной из таких поломок его не оказалось в городе. В результате конвейер завода остановился, а ущерб производству составил 170 не выпущенных автомобилей. Программист был привлечен к уголовной ответственности по ч. 2 ст. 98 УК РСФСР "Умышленное уничтожение или повреждение государственного или общественного имущества... причинившее крупный ущерб".

Выделяют следующие формы проявления компьютерной преступности.

1. Компьютерные манипуляции. Неправомочное изменение содержимого носителя информации и программ, а также недопустимое вмешательство в процесс обработки данных.

Для компьютерных манипуляций характерны некоторые особенности, обусловленные спецификой самого объекта преступных действий. Используется возможность отладки программ, составленных с преступными целями, многократная реализация однажды найденной возможности для незаконных действий. Противозаконные действия с системным программным обеспечением доступны только узкому кругу специалистов-программистов. Значительно меньший объем специальных знаний необходим для осуществления манипуляций с входными и выходными данными.

«Дело этого типа имело место в Лондоне. Группа мошенников объединилась с несколькими специалистами по компьютерам. Они обзавелись компьютером, сделали моделирующую программу в начали действовать по указанию из "штаб-квартиры", куда звонили по телефону и получали указания в соответствии с рекомендациями модели. Все шло блестяще, но тут произошел сбой в компьютере. Дублирующего компьютера не

предусмотрели, и "змей" рухнул. Скотланд Ярд за несколько дней арестовал всех мошенников. След естественным образом привел к "штаб-квартире", где специалисты по компьютерам, забыв о еде и сне, пытались наладить работу компьютера».

2. Хищение машинного времени, *т.е. использование компьютера в личных целях в рабочее время.*

3. Экономический шпионаж. Компьютерный шпионаж преследует, как правило, экономические цели. Преступления этой категории совершаются для получения следующей информации: программ обработки данных, результатов научных исследований, конструкторской документации и калькуляции, сведений о стратегии сбыта продукции и списков клиентов конкурирующих фирм, административных данных, сведений о планах и технологии производства.

4. Деятельность «хакеров» **или преступления** ***«со взломом».*** В общем виде используемая компьютерными преступниками методика «взлома» или несанкционированного доступа сводится к двум разновидностям:

а) «взлом изнутри»: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация, и может определенное время работать на нем без постороннего контроля;

б) «взлом извне»: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность проникнуть (обычно посредством удаленного доступа через компьютерные сети) в защищенную систему для внедрения специальных программ, проведения манипуляций с обрабатываемой или хранящейся в системе информацией или осуществления других противозаконных действий.

Компьютерные преступления отличаются от обычных особыми *пространственно-временными* характеристиками. Подобные деяния совершаются в течение нескольких секунд, а пространственные ограничения оказываются полностью устраненными.

Один из важнейших способов повышения эффективности борьбы с компьютерной преступностью - создание надлежащей правовой основы для преследования в уголовном порядке виновных лиц. Подготовка нормативно-правовых актов в этой области исключительно сложна, поскольку связана с технологией, опережающей нормотворческий процесс. Развитие законодательства не успевает за развитием техники и преступным использованием ее последних достижений [2].

В компьютерных преступлениях ЭВМ может быть как *объектом,* так и *субъектом* преступления.

В тех случаях, когда ЭВМ - объект преступления, т. е. ей наносится материальный ущерб путем физического повреждения, не возникает проблем с применением существующего законодательства.

Однако случаи, когда ЭВМ используется для совершения актов обмана, укрывательства или присвоения с целью получения денег, услуг, собственности и деловых преимуществ, представляют собой новые правовые ситуации. Характерными чертами таких преступлений, усложняющих расследование и предъявление обвинения по ним, являются:

- сложность обнаружения преступлений, связанных с использованием ЭВМ;

- большая дальность действия современных средств связи делает возможным внесение незаконных изменений в программу ЭВМ с помощью дистанционных терминалов либо закодированных телефонных сигналов практически из любого района;
- затруднения в понимании порядка работы ЭВМ в технологически сложных случаях;
- информация преступного характера, заложенная в память ЭВМ и служащая доказательством для обвинения, может быть ликвидирована почти мгновенно;
- обычные методы финансовой ревизии в случае этих преступлений не применимы, так как для информации используются электронные импульсы, а не финансовые документы.

Зарубежный опыт законодательного регулирования проблем защиты компьютерной информации выявил ряд характерных моментов.

1. Практически во всех странах законодательно установлена ответственность за нарушение порядка обработки и использования персональных данных.

2. Информационные (компьютерные) преступления расцениваются как представляющие особую опасность для граждан, государства и общества в целом; характеризуются значительно более жесткими мерами наказания, чем аналогичные преступления, совершаемые без использования компьютерной техники.

3. Квалифицируются как преступления также действия, создающие только предпосылки к нанесению ущерба (попытка, проникновения в систему, внедрение программы-вируса).

К базовым направлениям повышения эффективности контроля над компьютерной преступностью в Росси следует отнести:

- формирование целостной системы непрерывного отслеживания обстановки в сфере обеспечения информационной безопасности различных систем в стране и упреждающего принятия решений по выявлению и пресечению компьютерных преступлений;
- организация взаимодействия и координация усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;
- организация эффективного взаимодействия правоохранительной системы России с правоохранительными органами зарубежных стран, осуществляющими борьбу с компьютерными преступлениями;
- координация действий с общественными и частными организационными структурами (фондами, ассоциациями, фирмами, службами безопасности банковских и коммерческих структур), на своем уровне осуществляющими практические мероприятия по обеспечению информационной безопасности.

Создаваемая система должна быть обеспечена высококвалифицированными кадрами. Создание целостной системы обучения, подготовки и переподготовки специалистов по борьбе с компьютерными правонарушениями является одной из основных задач.

Список литературы

1. *Кантышев П.* Статистика киберпреступлений в России [Электронный ресурс] – Режим доступа: http://www.vedomosti.ru/tech/news/39108691/kiberprestupniki-v-spiskah-ne-znachatsya (дата обращения 20.02.2015).

2. *Красников А.Ф* Теневая экономика и экономическая преступность [Электронный ресурс] – Режим доступа: http://newasp.omskreg.ru/bekryash/index.htm (дата обращения 20.02.2015).