ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (КИБЕРПРЕСТУПНОСТЬ)

Василенко Н.А.

г. Воронеж, Муниципальное бюджетное учреждение дополнительного образования Центр дополнительного образования «Реальная школа», 10 класс

Научный руководитель: Енина Н.В., г.Воронеж, Муниципальное бюджетное учреждение дополнительного образования Центр дополнительного образования детей «Реальная школа» (МБУДО ЦДО «Реальная школа»), педагог

«По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, - но и в этом случае сомнения не оставляют меня».

Юджин Х. Спаффорд.
(эксперт по информационной безопасности)

Информационная преступность - это и кража денег, и распространение вредоносных программ (вирусов).

Сегодня проблема преступности в информационных технологиях является актуальной и достаточно болезненной, так как с развитием информационных технологий жестко развивается и вредоносная вирусная база, и сети взломщиков. Сегодня взлом паролей, кража номеров кредитных карточек, фишинг, неправомерное противозаконное распространение информации через глобальную сеть стали очень популярными и практически ненаказуемы.

Главной проблемой современности является уровень специальной подготовки должностных лиц правоохранительных органов.

Цель исследования состоит в изучении и анализе положений, характеризующих понятие «компьютерного преступления» и уголовно-правовой состав неправомерного доступа к информации, а также в выявлении недостатков в современном законодательстве устраняющих неопределенность знаний в сфере информационных правонарушений.

В соответствии с поставленной целью необходимо решить следующие **задачи:**

- изучить развитие преступлений в сфере высоких информационных технологий;
- рассмотреть понятие и дать общую характеристику преступлений в сфере компьютерной информации;
- исследовать законодательство России об уголовной ответственности за преступления в сфере компьютерной информации;
- дать уголовно-правовую характеристику преступлениям в сфере компьютерной информации;
- проанализировать проблемы, возникающие в области борьбы с компьютерными преступлениями и предложить пути их решения.

Характер решаемой проблемы, цели и задачи исследования определяют, каким должен быть объект исследования. **Объектом исследования** являются организационно-правовые отношения, складывающиеся в сфере охраны целостности компьютерной информации.

Предметом исследования является законодательство, направленное на борьбу с преступностью в сфере высоких информационных технологий.

Изучение темы работы основано на использовании таких научных методов исследования как: общетеоретический, анализ, синтез, логический, сравнительно-правовой, исторический, статистический, а также метод анализа и толкования правовых актов.

Нормативно-правовой основой исследования являются: Всеобщая декларация прав человека, Международная конвенция о пресечении обращения порнографических изданий и торговли ими, Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Федеральный закон «Об информации, информатизации и защите информации», Закон РФ «О государственной тайне» и некоторые другие нормативно-правовые акты.

В главе 28 УК РФ указаны следующие общественно опасные деяния в отношении средств компьютерной техники:

1. Неправомерный доступ к охраняемой законом компьютерной информации.

2. Нарушение правил эксплуатации ЭВМ, что приводит к уничтожению, блокированию или модификации охраняемой законом информации ЭВМ.

Появлению информационной преступности способствовало появление так называемых «хакеров» (hacker) – пользователей занимающихся изучением и поиском уязви-

мых мест компьютерных сетей, операционных систем и систем информационной безопасности. К хакерам можно отнести лица, важной особенностью которых является сочетание профессионализма в области программирования с элементами фанатизма и изобретательности. У преступников данной группы нет каких-либо ярко-выраженных намерений. Большая часть действий совершается ими с целью проявления своих интеллектуальных и профессиональных способностей.

Рассмотрим теперь мотивы и цели совершения компьютерных преступлений. Мотивы и цели совершения преступления напрямую связаны с социально-психологической и криминологической характеристиками личности преступника. Некоторые мотивы указаны в уголовном законе в качестве смягчающих обстоятельств (преступления вследствие стечения тяжелых личных или семейных обстоятельств, под влиянием угрозы или принуждения, либо материальной, служебной или иной зависимости, совершение преступления в состоянии аффекта или невменяемости и т.д.). Однако для большинства умышленных преступлений мотив и цель не является необходимыми элементами субъективной стороны и, следовательно, не входят в уголовно-правовую характеристику.

В связи с этим, представляется возможным остановиться на более узком сегменте информационной сферы - сфере компьютерной информации. Их, можно разделить на две категории (табл.1).

Таблица 1

Компьютерные преступления

Компьютер как объект преступления	Компьютер как орудие преступления
Хищение технических средств и компьютерной информации	Банковские хищения
Повреждение технических средств и компьютерной информации	Шпионаж (государственный, промышленный, коммерческий)
Несанкционированный доступ к техническим средствам и информационным ресурсам	Фальсификация результатов голосования

В первой категории компьютер и (или) компьютерная информация является объектом преступления. К этой категории относятся хищение или нанесение ущерба техническим средствам и информации, несанкционированный вредоносный доступ к компьютерной системе и информационным ресурсам.

Во второй категории компьютер служит орудием преступления. Таковы, например, осуществляемые с помощью компьютера банковские хищения; государственный, коммерческий, промышленный шпионаж; распространение компрометирующей информации, фальсификация результатов голосования и т.п. Обе категории преступлений тесно взаимосвязаны: например, компьютер может служить орудием несанкционированного доступа к другому компьютеру.

Это позволяет выделить среди преступлений, совершаемых с применением компьютерных технологий и использованием компьютерной информации, три категории преступлений:

- преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения, т.е. отношения, возникающие по поводу осуществления информационных процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, создания и использования компьютерных технологий и средств их обеспечения, а также защиты компьютерной информации, прав субъектов, участвующих в информационных процессах и информатизации;

- преступления в информационном компьютерном пространстве, посягающие на отношения возникающие по поводу реализации прав на информационные ресурсы (собственности и т.д.), информационную инфраструктуру и составляющие ее части (ЭВМ, системы и сети ЭВМ, программы для ЭВМ и т.д.);

- иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства при совершении деяний, посягающих на иные охраняемые уголовным законом правоотношения (собственности, общественной безопасности и т.д.).

Различают следующие группы преступлений.

Экономические преступления - самые распространенные, осуществляются с корыстными целями (мошенничество; хищение программ, услуг, компьютерного времени; экономический шпионаж).

Преступления против личных прав и частной сферы (сбор компрометирующих данных о лицах; разглашение банковской, врачебной и другой частной информации; получение данных о доходах или расходах).

Преступления против государственных и общественных интересов (ущерб оборо-

носпособности, фальсификация результатов голосования).

К преступному вмешательству в работу компьютера относится:

Несанкционированный доступ к компьютерной информации в корыстных целях. При этом может использоваться чужое имя, изменение физических адресов технических устройств, остаточная информация, модификация информации и программного обеспечения, подключение записывающих устройств к каналам связи, маскировка под законного пользователя путем раскрытия его пароля (если нет средств аутентификации). При наличии незащищенных файлов несанкционированный доступ возможен и вследствие поломки.

Разработка и распространение «компьютерных вирусов», которые могут распространяться и заражать другие компьютеры; «логических или временных бомб», которые срабатывают при определенных условиях или по достижении определенного времени и полностью или частично выводят из строя компьютерную систему, а также «червей».

Халатная небрежность при разработке и эксплуатации программного обеспечения компьютерной системы, которая может привести к тяжелым последствиям. Но полной надежности быть не может, в программах всегда могут остаться незамеченные ошибки.

Подделка и фальсификация компьютерной информации. Например, при выполнении контрактных работ можно таким путем выдать вновь разработанные негодные компьютерные системы и программное обеспечение за годные и сдать заказчику. Можно фальсифицировать результаты выборов, референдумов, опросов. Возможна и фальсификация в корыстных целях.

Хищение программного обеспечения. В РФ значительная часть программного обеспечения распространяется путем краж, продажи краденого, обмена краденым. Таковы, например, известные «пиратские» компакт-диски, которые значительно дешевле лицензионных и поэтому широко применяются пользователями компьютеров. Бороться с этим видом хищений очень трудно.

Несанкционированное копирование, модификация, уничтожение информации. Преступное присваивание информации может осуществляться путем копирования. Информация должна представлять собой самостоятельный объект охраны.

Несанкционированный просмотр или хищение информации из баз данных, банков данных, баз знаний.

Одним из важных элементов обеспечения информационной безопасности является защита интеллектуальной собственности. Актуальность проблемы обусловлена тем, что, во-первых, информационная сфера насыщена технологиями, которые являются объектами интеллектуальной собственности. Закрепление прав на информационные технологии и защита этих прав являются базисом для развития отношений в данной сфере. Во-вторых, в результате некоторой финансовой стабилизации, позволившей накопить стартовые бюджетные ассигнования для поддержки инноваций, экономика страны переходит на инновационный путь развития. Неотъемлемым условием этого перехода является эффективная защита прав на объекты интеллектуальной соб-

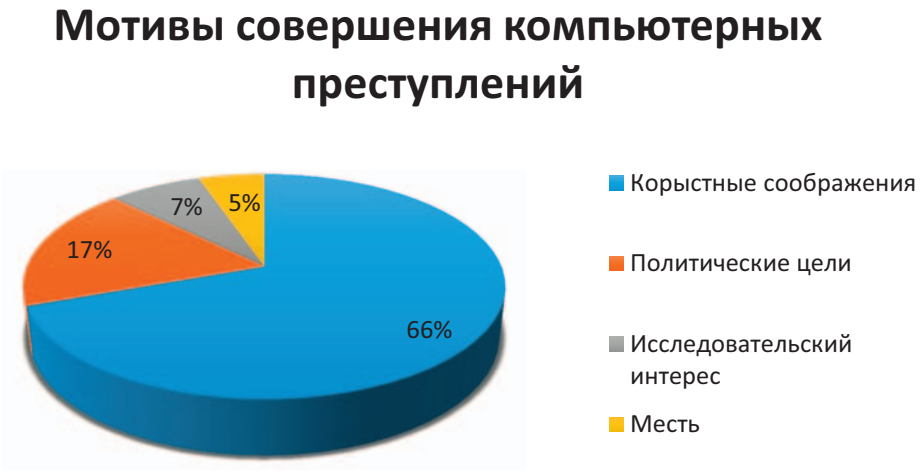

Рисунок 1. Диаграмма мотивов совершения компьютерных преступлений

ственности, что особенно важно для военно-технического комплекса.

Исходя из результатов изучения зарубежных исследователей по этому вопросу, в настоящее время можно выделить, пять наиболее распространенных мотивов совершения компьютерных преступлений, представленных в следующей диаграмме:

Как правило, 52% преступлений связано с хищением денежных средств; 16% - с разрушением и уничтожением средств компьютерной техники; 12% - подменой данных;10% - с хищением информации и программного обеспечения; 10% - связанно с хищением услуг.

Профилактика компьютерных преступлений

Почти все виды информационных преступлений можно, так или иначе, предотвратить. Для решения этой задачи правоохранительные органы должны использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению.

На основе данных, полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с компьютерной преступностью, можно выделить три основные группы мер предупреждения компьютерных преступлений:

1) правовые;

2) организационно-технические;

3) криминалистические.

Подводя итоги, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК.

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 не раскрываемо, 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.

Список источников

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).

2. Кодекс Российской Федерации «Об административных правонарушениях» от 30.12.2001 №195-ФЗ (ред. от 27.07.2010).

3. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (с послед. изм. и доп.)

4. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с послед. изм. и доп.).

5. Вехов В. Б. Компьютерные преступления// М.: Право и Закон, 1996Волеводз А.Г. Правонарушения в информационной сфере: некоторые проблемы ответственности.

6. А.Г.Волеводз // Информационное общество в России: проблемы становления. - М.: МИРЭА, 2002. - С. 26-35.

7. Копылов В.А. Информационное право. Учебник / В.А.Копылов. - М.: Юристь, 2002. - 512 с.

8. Королев А. Комментарий к ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный) / А.Королев, О.Плешакова. - М.: Юстицинформ, 2009.