**ИСТОРИЯ ПОЯВЛЕНИЯ И РАЗВИТИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры, хищения наличных и безналичных денежных средств. Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Так, по мнению начальника отдела по делам о преступлениях в сфере экономики и компьютерной информации Контрольно-методического управления Следственного комитета при МВД РФ Г.Егорова, в СССР первое преступление было совершено в 1979 году в Вильнюсе. Ущерб государству тогда составил 80 тысяч рублей - на эти деньги можно было приобрести 8 автомобилей "Волга". В 2007 году в сфере высоких технологий на территории России было зафиксировано уже 300 преступлений, а в 2000 году - более 1300. На Украине в 2002 году было возбуждено 31 уголовное дело, из которых 29 на настоящий момент окончены производством. С начала 2003 года на Украине возбуждено уже 10 уголовных дел рассматриваемой категории. В Казахстане до 2002 года было зарегистрировано всего 17 сходных преступлений.

Жертвами преступников становятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Чаще всего мишенями преступников становятся банки. Особая актуальность вопросов защищенности технических средств приема, передачи и накопления информации от несанкционированного доступа была отмечена и отечественным законодателем, в частности законом РК №233-1 "О национальной безопасности" от 26 июня 2008 года введением понятия "информационная безопасность".

Остается актуальной проблема борьбы с организованной преступностью, которая, прибегая к услугам высококвалифицированных специалистов, стала все чаще использовать различные технические средства - от обычных персональных компьютеров и традиционных средств связи до сложных вычислительных систем и глобальных информационных сетей, в том числе и Интернет. Сфера применения компьютерных технологий в преступных целях весьма обширна. Так, по данным ОКУ ГУВД г.Алматы, практически каждый второй поддельный денежный знак изготавливается с использованием компьютерной обработки и распечатки на цветном принтере. Объясняется это, прежде всего общедоступностью такого рода информационных технологий и простотой их эксплуатации.

Компьютерно-информационные технологии функционируют относительно давно, и их развитие происходит огромными темпами, что связано с большой заинтересованностью ими широких слоев населения. Преступления, связанные с использованием компьютерной техники, - это лишь специализированная часть преступной деятельности в информационной сфере. К данной категории относятся и преступления, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. С закреплением в Уголовном кодексе Республики Казахстан в ст.227 состава преступления, предусматривающего ответственность за такого рода деяния, правоохранительные органы получили реальное средство борьбы с лицами, использующими компьютерную технику в преступных целях.

Огромен и вред от такого рода преступлений. По оценкам специалистов, в среднем экономический ущерб только от одного такого преступления в США составляет 450 тыс. долларов. Ежегодные же потери оцениваются: в США - 100 млрд. долларов; в Великобритании - 4,45 млрд. долларов; в странах Западной Европы - 30 млрд. долларов. Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Кроме того, следует отметить, что подобные преступления все чаще совершаются сотрудниками фирмы, банка или другого учреждения, которым в конечном итоге и наноситься ущерб. Например, в США компьютерные преступления, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами. В Казахстане то же существует такая тенденция. Так, в 2000 году в Лондоне были арестованы О. Зезов и И. Яримак, граждане Казахстана, по обвинению в неавторизированном компьютерном проникновении, заговоре, нанесении вреда комерции путем вымогательства и попытке нанесения вреда путем вымогательства с использованием корпоративной информации компании Bloomberg LP. Сумма шантажа составляла 200 тысяч долларов. Оба казахстанца были арестованы в аэропорту в момент передачи денег. Примечательно, что оба они работали в компании, производящей базы данных для Bloomberg LP, и воспользовались полученной в ходе этого информацией для достижения своих преступных целей. Суд над ними состоялся лишь летом 2002 года, исходя из сложности доказывания такого преступления. В США, где проходило судебное разбирательство, максимальный срок наказания по совокупности за эти преступления составляет 28 лет.

Для того чтобы понять, что же представляет собой "охраняемая законом компьютерная информация", мы приведем краткий перечень некоторых видов информации, охраняемых законодательством Республики Казахстан, которые одновременно подлежат защите. Этот перечень выделен отечественным ученым Ж. К. Амановым:

- государственные секреты;

- служебная и коммерческая тайна;

- банковская тайна;

- нераскрытая информация;

- личная и семейная тайны, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

- тайна усыновления (удочерения) ребенка;

- адвокатская тайна;

- тайна пенсионных накоплений получателя.

Таким образом, "охраняемая законом компьютерная информация", по мнению Ж. К. Аманова, позицию которого мы полностью разделяем, есть сведения, данные, знания, дающие представление о каком-либо явлении или предмете, охраняемые действующим законодательством, находящиеся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

По свидетельству специалистов, наиболее привлекательным сектором экономики практически любой страны является ее кредитно-финансовая система. Наиболее распространенным в этой области являются компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей. В России, например, только за 2008 год было выявлено 15 подобных преступлений, в ходе расследования которых были установлены факты незаконного перевода 6,3 млрд. рублей. Вообще, в 2008 году в России было возбуждено 39 уголовных дел в области злоупотребления компьютерной информацией, тогда как в 2007 году – всего лишь 9 уголовных дел. В целом, в Российской Федерации в настоящий момент завершено производством около 100 уголовных дел, предусмотренных главой 28 Уголовного кодекса РФ. В Казахстане таковых дел единицы.

Однако компьютерная техника и средства коммуникаций на территории Республики Казахстан используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение машинного времени, а также денежных средств посредством электронной транзакции - вот далеко не полный перечень преступлений, с которыми вынуждены бороться правоохранительные органы США, Канады, стран Европы и т.д.), а в большей степени как средства преступной деятельности. Причина - высокая латентность данного вида преступлений и слабо развитые, а иногда даже отсутствующие компьютерно-информационные сети. За рубежом, например, активно борются с проблемой латентности. Так, по данным Института компьютерной безопасности США (Computer Security Institute, CSI) из Сан-Франциско, число компаний, сообщавших о компьютерных преступлениях в отношении той или иной их формы, выросло с 2008 по 2001 год почти вдвое - с 17 до 32%.

Еще одна из причин роста таких преступлений в Казахстане – это разрыв в уровнях развития информационного общества по сравнению с Западом, порождающий иногда абсурдные ситуации, нестыковки моральных, правовых стандартов и норм. Создаются условия для соблазна, искушения воспользоваться более удобной и дешевой формой обеспечения информацией. Взять, например, проблему сохранения интеллектуальной собственности. Лицензионные программы стоят очень дорого для массового потребителя и нет моральных преград пользоваться «взломанными» программами, которые во много раз дешевле.

Как показывает практика показывает, что буквально единицы уголовных дел, возбужденных на территории стран бывшего Советского Союза, по сравнению с западными странами, связаны с незаконным доступом к охраняемой законом компьютерной информации, тогда как в большем количестве дел электронная информация фигурирует в качестве доказательств. Как отмечает В.Б. Крылов, правоохранительным органам становится известно не более 5-10% совершенных компьютерных преступлений. Это связано с тем, что хищение информации долгое время может оставаться незамеченным, поскольку зачастую данные просто копируются. Жертвы компьютерной преступности (большинство из них частные предприниматели) проявляют нежелание контактировать с правоохранительными органами, опасаясь распространения среди вкладчиков и акционеров мнения о собственной халатности и ненадежной работе своей фирмы, что может инициировать отток финансов и последующее банкротство. Например, в Англии преступникам было выплачено 400 миллионов фунтов стерлингов в качестве отступного за обещание не поднимать шума. Преступники осуществили электронное проникновение в ряд банков, брокерских контор и инвестиционных компаний Лондона и Нью-Йорка, установив там программы – вирусы, активизирующиеся по желанию преступников. Банки предпочли удовлетворить требования вымогателей, поскольку огласка случаев электронного взлома могла бы поколебать уверенность клиентов в безопасности банковских систем.

Если же в России одним из первых наиболее крупных компьютерных преступлений считается уголовное дело о хищении 125,5 тыс. долл. США и подготовке к хищению еще свыше 500 тыс. долл. во Внешэкономбанке СССР в 2001 году, то в Казахстане первое наиболее крупное преступление с использованием компьютерных технологий имело место в 2004 году (хотя такие преступления были зафиксированы и ранее - дело на "Автовазе", хищения в Вильнюсе в 80-е годы). Тогда это было первое уголовное дело против бывшего оператора Алатауского филиала КРАМС - банка г. Алматы Э. Р. Ордабаева, который путем использования ключевой шифровальной дискеты осуществил две фиктивные бухгалтерские проводки на сумму 6 млн. 795 тыс. тенге на счет малого предприятия "Анжелика".

Одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет (International Network – международная система связи). В настоящее время Интернет, использующая в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками, объединяющую около 30 000 мелких локальных сетей и более 30 миллионов пользователей, число которых постоянно растет. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных минипроцессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам интернет позволяет передавать не только аудио, но и видео, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, - воз­можность осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма за­интересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. Кроме того, существует проблема распространения в сети информации порнографического характера, которая, согласно ст.273 Уголовного кодекса Республики Казахстан, является уголовно-наказуемым деянием. Вот только несколько примеров из международной практики:

- осенью 2008 года полицейские органы 12 стран мира в ходе совместной операции «Собор» арестовали 107 членов закрытого Интернет - клуба «Страна чудес», имевших доступ к 100 тысячам файлов детской порно­графии. План операции придумали британцы, задержавшие 11 интернет - педофилов и раскрывшие их базу в Сассексе. По этому делу в США было арестовано 32 человека, в Германии - 18, в Италии - 16. По итогам операции «Собор» осенью 2000 года в Велико­британии появился спецотдел «компьютерной полиции» по борьбе с интернет - маньяками и хакерами;

- в сентябре 2000 года итальянские правоохранительные органы поместили в Интернете «порносайт», на который «клюнули» 500 человек. В их проверке участвовал известный эксперт по детской порнографии сицилийский священник Фортунато ди Нато. С его помощью в Риме и Неаполе были арестованы 8 порноторговцев, уничтожена их общая база данных - платный сайт «Холдинг» и выявлены трое постав­щиков порнофильмов из России, позднее арестованных на родине;

- С. Савушкин и О. Пьяницкий, жители России, находясь в Ростове-на-Дону, открыли порносайт на сервере Paradise Web Hosting в Америке. Банковский счет был открыт в Real Internet Company Inc. в Канаде. Переведя на этот счет от 9 до 25 долларов в качестве абонентской платы, любой человек мог ознакомиться с порнографической информацией самого различного характера. В ходе оперативно - следственных мероприятий по виртуальному адресу был вычислен реальный адрес одного из злоумышленников, и вскоре оба они были задержаны. Их доходы составили 1-2 тысячи долларов в месяц, однако эта цифра лишь то, что удалось доказать следствию. Реальные цифры скрыты за тайной канадских банковских вкладов.

Особо следует отметить опыт зарубежных стран для борьбы с такими преступлениями. Так, в США в "компьютерной столице" страны - Сан-Хосе в штате Калифорния Федеральное бюро расследований объединило службы, занимающиеся расследованием компьютерных преступлений, в единую бригаду, что существенно повысило не только уровень раскрытия преступлений, но и сделало возможным практически мгновенную реакцию ФБР не только на заявления о данных преступлениях, но и на самостоятельное их выявление. Однако не всегда уровень подготовки соответствующих специалистов для правоохранительных органов соответствует уровню отдельных преступников. Поэтому все чаще правоохранительные органы прибегают к помощи других лиц или даже организаций. Так, в Великобритании существует компьютерная фирма «Вогон Интернэшенел», сотрудники которой занимаются поисками следов преступления – выявления и исследования компьютерных данных, которые преступники пытаются уничтожить в целях маскировки преступления и затруднения поиска преступников.

Следует отметить, что понятие «компьютерных» или же «информационных» преступлений базируется исключительно на действующем уголовном законодательстве в этой области. Действительно, в России, например, глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации» предусматривает три состава преступлений - ст.272-274, в Республике Казахстан – один состав преступлений – ст.227 Уголовного кодекса РК. Название соответствующей главы в Уголовном кодексе РФ некоторые российские ученые связывают с тем, что в формулировании соответствующих составов преступлений законодателем акцент был сделан на защиту именно самой компьютерной информации, хотя и признают, что название главы является в известной мере условным. Вместе с тем в ходе проведенного нами анализа действующего в Казахстане уголовного законодательства было установлено, что при совершении ряда других преступлений могут использоваться информационные технологии, и как показывают приведенные выше примеры различных тенденций развития подобных преступлений, используются они преступниками довольно эффективно. Приведем перечень некоторых действий преступников, использующих информационные технологии, и соответствующие им составы преступлений, предусмотренных в законодательстве РК:

1. Распространение через каналы сети Интернет и местных локальных сетей:

- заведомо ложных сведений, порочащих честь и достоинство лица или подрывающих его репутацию – ст. 129 УК РК «Клевета»;

- информации, связанной с унижением чести и достоинства лица, выраженной в неприличной форме - ст. 130 УК РК «Оскорбление»;

- сведений о частной жизни лиц, составляющих их личную или семейную тайну – ст. 142 УК РК «Нарушение неприкосновенности частной жизни», тайну переписки, телефонных переговоров, почтовых, телеграфных или других сообщений – ст. 143 УК РК «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;

- информации, призывающей к развязыванию агрессивной войны – ст. 157 УК РК «Пропаганда и публичные призывы к развязыванию агрессивной войны», к насильственному изменению государственного строя – ст. 170 УК РК «Призывы к насильственному свержению или изменению конституционного строя либо насильственному нарушению единства территории Республики Казахстан», составляющей государственную тайну – ст. 172 УК РК «Разглашение государственной тайны» и т.п.;

- информации порнографического характера – ст. 273 УК РК «Незаконное распространение порнографических материалов и предметов».

2. Мошенничество в сфере использования азартных игр (казино, лотереи и тотализаторы), организации финансовых пирамид, фиктивных брачных контор и фирм по оказанию несуществующих услуг – ст.177 УК РК «Мошенничество».

3. Получение вознаграждения за неразглашение сведений, полученных в ходе несанкционированного доступа к информации, составляющей коммерческую или банковскую тайну, – ст.181 УК РК «Вымогательство», ст. 200 УК РК «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну».

4. Незаконное копирование и продажа программных продуктов, находящихся на серверах компа­ний, которые являются владельцами этих программ, с присвоением их авторства другим лицом либо компанией – ст. 184 УК РК «Нарушение прав интеллектуальной собственности», а также использование преступником логотипа или наименования товара другой фирмы – ст.200 УК РК «Незаконное использование товарного знака».

5. Изготовление с использованием средств компьютерной техники поддельных денежных знаков и документов – ст. 206 УК РК «Изготовление или сбыт поддельных денег или ценных бумаг», ст. 207 «Изготовление или сбыт поддельных платежных карточек и иных платежных и расчетных документов», ст.208 УК РК «Подделка и использование марок акцизного сбора» и т.п.

Таким образом, уголовная ответственность за использование информационных технологий для совершения преступлений охватывает довольно большой перечень общественных отношений, гораздо обширнее, на наш взгляд, чем отношения в области компьютерной информации, но менее обширный, чем информационные отношения.

Очевидно, что частная методика расследования подобных преступлений не будет являться основной, предпочтение будет отдано специальным методикам расследования, построенным не по видам преступлений, а по другим основаниям. Анализ вышеизложенного позволяет указать в качестве оснований для выделения частной специальной методики расследования преступлений в рассматриваемой области преступную сферу использования информации в электронном виде. Кроме того, к основаниям могут быть отнесены и отдельные элементы криминалистической характеристики подобных преступлений, такие как объект посягательства, орудия и средства совершения этих преступлений, в качестве которых выступают устройства сбора, хранения и обработки информации, а также способы их совершения. Наряду с этим в качестве основания для выделения частной специальной методики выступает и характер специальных знаний, используемых при расследовании подобных преступлений, которые, как справедливо отмечает отечественный ученый А.А.Исаев, используются при квалификации преступлений при установлении элементов состава преступлений. Так, путем привлечения специальных научных знаний в ходе расследования таких преступлений возможно установление предмета преступления, который в обобщенном виде для всей рассматриваемого вида преступлений представляет собой информацию в электронном виде и созданные на основе ее предметы реального мира или же совершенные в соответствии с ней какие-либо преступные деяния.

В результате анализа приведенных позиций и точек зрения можно определить данный вид преступлений как преступления в сфере высоких информационных технологий, под которыми понимается совершение противоправных деяний в области информационных отношений, осуществляемых посредством высокоточного оборудования и устройств, использующих технологию оперирования информацией. Данный термин наиболее точно определяет преступления в рассматриваемой нами области. Расследование преступлений, совершенных с использованием средств компьютерных технологий, в таком случае будет являться составной частью расследования преступлений в сфере высоких информационных технологий (ВИТ).

**Литература**

1. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs // Gazeta.Ru.- 2001.- 18 июня.
2. Закон Республики Казахстан «О национальной безопасности» // Нормативные акты. – Алматы: Аян Эдет, 2008.- С.47.
3. Крылов В.В. Информация как элемент криминальной деятельности // Вестник Моск. ун-та. Сер. 11. Право. - М., 2008.-№4.-С.50-64.
4. Уголовное право. Особенная часть: Учебник для вузов / Под ред. Н.И.Ветрова, Ю.И.Ляпунова. – М.: Новый юрист, 2008.–768с.
5. См. подробнее: Форпост.-2002 .- 4 июня,- №19(70).
6. См. подробнее: Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: Сб. матер. межд. конф. 1 – 2 марта 2001 г. – Алматы: Интернет трейнинг центр, 2001.
7. См. подробнее: Информация о преступлениях в сфере высоких технологий. – М.: ГИЦ МВД РФ, 2009.
8. См. подробнее: Катаев С.Л. Социальные аспекты компьютерной преступности // Центр иссл. пробл. комп. преступн. – Киев, 2002.
9. Крылов В.Б. Информационные компьютерные преступления. – М.: ИНФРА-М-НОРМА, 2007.
10. Анин Б. Защита компьютерной информации. – СПб.: BHV, 2000.
11. London Times.- 2006.-3 June.
12. См. подробнее: Оспанов Е.Т. Орудие преступления – компьютер // Бюллетень ГСУ и ЭКУ МВД РК. – Алма-Ата: МВД РК, 2005.- №1-2(1-5).-С.35-41.
13. См. подробнее: Ладный В. Чтоб сайт стоял и деньги были // Комсомольская правда. - 2001.- 26 января, - №14(22479).
14. См. подробнее: Исаев А.А. Применение специальных познаний для квалификации преступлений. – Алматы: Мектеп, 2007.