В.К. Гавло, В.В. Поляков

Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации

В России происходит процесс освоения и применения преступниками новых компьютерных и информационных технологий, используемых ими в качестве средств совершения преступлений. В настоящее время темпы роста преступлений в сфере компьютерной информации с каждым годом увеличиваются [1]. Эти преступления ранее не были известны отечественной юридической науке. Уголовно-правовая охрана компьютерной информации началась с 1997 г., когда был принят новый Уголовный кодекс (УК) РФ*. В связи с этим понимание особенностей и механизмов совершения таких преступлений является актуальной задачей, важной как для их расследования, так и для предотвращения. В настоящей работе проведено обобщение типичных черт наиболее распространенных преступлений, связанных с неправомерным доступом.

Обобщенные нами материалы расследования по Алтайскому краю за 2004–2005 гг. свидетельствуют о том, что они осуществлялись следователями управления ГУВД Алтайского края. В состав следственной группы в большинстве случаев привлекались специалисты и эксперты в области средств компьютерной техники и компьютерной информации. По изученным нами материалам судебно-следственной практики около 85% уголовных дел были переданы в суд, а оставшиеся на стадии следствия были прекращены за деятельным раскаянием и примирением сторон. Наиболее распространенным видом преступлений из возбужденных уголовных дел был неправомерный доступ к сети Интернет.

При исследовании данной категории дел следствие затруднялось с ответами на вопросы установления способов их совершения, личности преступника, поиска доказательств, их оценке и использования в процессе доказывания как на предварительном следствии, так и в суде.

Способы совершения преступлений, связанных с неправомерным доступом к информации

Обобщение практики расследования уголовных дел, возбужденных по ст. 272 УК РФ, позволяет выделить типичные способы и механизмы совершения данных преступлений. Суть их в следующем.

Вариант 1. На подготовительном этапе совершения преступлений преступники четко определяли цель посягательства – завладение учетными записями законных абонентов провайдеров, т.е. их логином (именем пользователя) и паролем. Затем планировали техническую сторону совершения преступления. В соответствии с заранее определенным планом подыскивались соответствующие программные средства и инструкции к ним, с помощью которых была бы возможна реализация задуманного. Следует отметить, что программ для похищения чужих учетных данных существует достаточно много. Их можно легко приобрести в отделах по продаже компьютерных дисков или скопировать из Интернета, где они находятся в открытом доступе. Получение пароля возможно также путем самостоятельного составления программы автоматического набора необходимого номера и перебора возможных паролей. Для их составления требуется невысокий уровень знаний программирования.

Далее, при использовании преступных средств происходило непосредственное воплощение умысла – воздействие на информацию в объекте преступного посягательства. Оканчивалось преступление достижением желаемого результата, заключающегося в неправомерном доступе к информации и ее копировании.

Вариант 2. Следует отметить, что в рассмотренных типичных способах и механизмах совершения преступлений, связанных с неправомерным доступом к информации, отсутствовали некоторые характерные для такого рода преступлений элементы. Так, преступниками не был осуществлен этап предварительного сбора информации об объекте преступного посягательства, организации его работы и технологии обработки информации на нем, характеристиках и составе используемого обеспечения, в том числе программ по информационной безопасности. Преступники не выбирали конкретного пользователя или ЭВМ, с которой будет похищена информация. Логического завершения способа со-

* Здесь и далее под компьютерной информацией понимается информация на машинном носителе, электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

вершения преступления в виде сокрытия виртуальных и традиционных следов также не происходило.

Основным этапом данных преступлений, позволяющим проникать в сеть Интернет за счет средств законного пользователя, являлось получение логина и пароля. Способы похищения учетной записи, по нашему мнению, можно подразделить на два вида.

1. Совершение данных преступлений осуществлялось традиционным путем, т.е. путем похищения, мошеннических действий. В таких ситуациях преступники тайно копировали логин и пароль потерпевших, находящихся совместно с ними в квартирах, офисах, иных помещениях. В другом случае преступник получил логин и пароль унитарного государственного предприятия от неустановленного лица, похитившего их.

2. Данные преступления совершались с использованием специальных технических и программных средств, а именно вредоносных компьютерных программ, позволявших незаконно проникать на сервер провайдеров (провайдер – фирма, предоставляющая пользователям доступ в Интернет), в ЭВМ граждан и организаций, систему ЭВМ или их сеть. Так, группа лиц в составе студента вуза и учащегося школы посредством вредоносной программы «AntiLamerBackDoor v.1.4» неоднократно копировала с электронного почтового ящика на сервере провайдера на жесткий диск компьютера учетные записи потерпевших.

После того, как учетные записи пользователей (клиентов фирмы провайдера) были добыты, осуществлялось незаконное проникновение в сеть Интернет. Преступники использовали персональные компьютеры, находящиеся в их собственности. Системные блоки этих компьютеров соединялись при помощи модема с телефоном и телефонной линией. Такое соединение обеспечивало подключение к сети Интернет через сервер конкретного провайдера. Для этого запускалась программа, установленная на компьютере, обеспечивающая соединение компьютера с сервером доступа в Интернет. После установления соединения с компьютера вводились похищенные логин и пароль законного пользователя. Это обеспечивало свободный доступ к информации, находящейся как в сети Интернет, так и на сервере провайдера. На заключительном этапе полученная в результате неправомерного доступа информация записывалась на жесткий диск компьютера.

С точки зрения технических особенностей неправомерное получение информации достигалось с помощью удаленно расположенного компьютера по информационной сети. Преступники имели возможность выбора места и времени совершения преступления. Отметим также другие общие черты рассматриваемых преступлений. Они совершались неоднократно – десятки и даже сотни раз, и на протяжении длительного времени, как правило, одного–двух месяцев.

Поясним существенные принципы работы провайдеров. Интернет-провайдер в соответствии с регламентом регистрирует клиента. После регистрации он присваивает ему индивидуальные данные, позволяющие идентифицировать компьютер клиента. Услуги пользования ресурсами Интернета – платные. Оплачивается, как правило, время пребывания в сети и (или) объем полученной клиентом информации. Логин и пароль пользователя находятся на сервере (специально используемом для управления сетью компьютере провайдера). Для вхождения в сеть достаточно указать логин и пароль. За полученные услуги согласно прейскуранту автоматически снимается соответствующая часть оплаты, ранее перечисленной клиентом.

Именно эти обстоятельства делают хищение учетных записей основным элементом преступления. Они создают предпосылки преступления и делают его возможным. На наш взгляд, хищению индивидуальных учетных записей не уделяется необходимого внимания. Более того, сам этот факт, не окончившийся неправомерным доступом к информации, не рассматривается как подготовка к совершению преступления, что совершенно неправильно. Такой пробел в законодательстве способствует совершению подобных преступлений.

Таким образом, в рассмотренных нами преступлениях, как правило, имелись следующие последовательно развивающиеся общие черты.

1. Осуществление неправомерного доступа к информации дистанционным методом.

2. Модификация компьютерной информации, находящейся в закрытом доступе на сервере интернет-провайдера в виде изменений на счетчиках времени и объема полученной информации законного пользователя, а также его лицевом счете, в котором детализировалась информация о сумме, оставшейся на его балансе.

3. Блокирование компьютерной информации, так как во время неправомерного пребывания преступника в сети Интернет законный владелец был лишен доступа к серверу провайдера.

4. Копирование неправомерно полученной информации из сети Интернет на собственный персональный компьютер для ее дальнейшего использования.

Особенности личности преступников, совершавших неправомерный доступ в Интернет

Лица, совершавшие преступления, обладали некоторыми схожими чертами, знание и осмыс-

ление которых способствует как раскрытию таких преступлений, так и их профилактике. Это связано с тем, что данная информация может скорректировать криминалистическую характеристику преступлений, связанных с неправомерным доступом к компьютерной информации в части ее основного элемента – типовой характеристики личности преступника. В дальнейшем использование полученных научных знаний на практике позволит сузить поиск преступников и ориентировать на конкретные способы их эффективного изобличения [2].

Классифицируя преступников по рассматриваемой нами категории дел в зависимости от доминирования мотива преступления, их условно можно подразделить на два типа. Первые стремились извлечь материальную выгоду, безвозмездно пользоваться услугами провайдеров, вторые – преследовали исследовательскую цель и желание оценить уровень своих специальных знаний, при этом также не оплачивая услуги провайдера. С представителями второго типа преступников легче установить психологический контакт и больше вероятность, что они окажут содействие следствию. Значение цели и мотива, которые движут преступником, выражается в том, что они несут на себе субъективный отпечаток в выборе способа достижения преступного результата, который в конечном счете определяется конкретными свойствами личности. Зная эти свойства, можно обоснованно выдвигать следственные версии о том, каким способом было совершено преступление и какие следы преступления необходимо искать.

Данные преступления, как правило, совершались в одиночку, при этом преступники не вели активную социальную жизнь. Из рассмотренной группы преступлений в качестве преступников выступали исключительно мужчины, преимущественно в возрасте от 17 до 30 лет. Среди них учащиеся ПТУ и школ, студенты вузов, а также лица, имеющие высшее образование. Совершавшие данные преступления лица ранее были не судимы и, как правило, при судебном разбирательстве характеризовались положительно. При этом каждый из преступников знал о правилах пользования сетью Интернет, в частности, то, что любой пользователь обязан оплачивать услуги провайдера. Кроме того, все они заведомо осознавали свои преступные намерения, заключавшиеся в уклонении от уплаты услуг доступа в Интернет и причинении имущественного ущерба законным абонентам, со счетов которых без их ведома снималась оплата. Отметим, что совершавшим преступные деяния лицам было безразлично, за счет чьих средств они осуществляли неправомерный доступ к информации. Все они обладали навыками работы с персональным компьютером и его программным обеспечением. Однако уровень специальных знаний у каждого из них был невысокий. Это способствовало тому, что преступники, как правило, не скрывали совершенные ими преступления, активно шли на контакт и содействие следствию, в большинстве случаев сразу же признаваясь в содеянном. Следственные ситуации характеризовались как бесконфликтные.

Доказательства и доказывание при расследовании преступлений, связанных с неправомерным доступом компьютерной информации

По всем уголовным делам обвинение обоснованно выдвигалось по ст. 272 УК РФ. Преступления заключались в неправомерном доступе к охраняемой компьютером информации, т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, когда это деяние повлекло уничтожение, блокирование, модификацию или копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Как было показано выше, при неправомерном доступе к сети Интернет действительно имеют место одновременно модификация информации на сервере интернет-провайдера, блокирование информации в виде лишения законного владельца доступа к информационным ресурсам и копирование информации, неправомерно полученной в сети Интернет.

При расследовании преступлений, связанных с неправомерным доступом к информации в сети Интернет, в качестве доказательств использовались как традиционные следы (следы-предметы, следы-вещества и следы-отображения), так и связанные со спецификой компьютерных преступлений виртуальные следы. Традиционными были следы, обнаруженные в месте нахождения компьютера, с которого происходил неправомерный доступ. По ряду уголовных дел неотложные следственные действия в виде осмотра, обыска и выемки дали следующие результаты. На рабочем месте были обнаружены следы преступника, документация по использованию программных средств, позволяющих осуществить неправомерный выход в Интернет, на средствах вычислительной техники были оставлены отпечатки пальцев рук, волосы и иные микрочастицы. Данные следы были изъяты и сохранены. Далее, все они успешно были применены и истолкованы при содействии специалистов в качестве доказательств в суде [3]. В качестве традиционных доказательств также широко применялись показания свидетелей и потерпевших. Свидетеля-

ми давались показания о времени, месте, лице, совершившем преступление, и других известных им событиях и фактах. Потерпевшие подтверждали, что заплаченные ими суммы по оплате услуг интернет-провайдеров превышали реальный объем услуг, полученных в соответствии с прейскурантом, а также факт блокирования выхода в Интернет.

Для доказывания в суде совершения преступлений, связанных с неправомерным доступом в Интернет, обвинению необходимо использовать, помимо электронных вещественных доказательств, также электронные документы, в которых содержится информация о преступлении [4]. Следует отметить выявленные особенности следов, которые ряд авторов справедливо предлагает назвать виртуальными [5]. К ним можно отнести то, что они обезличены, а также легко копируются, модифицируются, уничтожаются и обрабатываются, причем исключительно с помощью средств вычислительной техники. Эти следы также могут находиться на значительном расстоянии друг от друга. Так, на жестких дисках ЭВМ, изъятых в ходе следствия, хранились учетные записи законных пользователей, а также установленные вредоносные программы и программы, используемые для подключения к сети Интернет. Кроме того, в компьютерах и в серверах провайдеров были найдены данные о времени нахождения преступников в сети Интернет, объеме полученной информации, а также используемые характеристики соединения их компьютеров с серверами провайдеров по телефонной сети с конкретных телефонов. При расследовании данных преступлений организации, предоставляющие услуги доступа в Интернет, оказывали следствию необходимую помощь.

При доказывании рассматриваемых преступлений необходимо учитывать специфику объекта преступлений, в качестве которого выступает компьютерная безопасность. Отсюда обоснованно выдвигается мнение, что преступление отсутствует, если в результате деяния, связанного, например, с копированием информации, не было и не могло быть причинено вреда [6]. В то же время при судебном разбирательстве необходимо учитывать, что дополнительным объектом неправомерного доступа к компьютерной информации являются материальные интересы потерпевших [7]. Принципиальным, на наш взгляд, является вопрос об имущественном ущербе, наносимом законному пользователю в результате ознакомления, модифицирования, блокирования, копирования, уничтожения компьютерной информации или нарушения работы ЭВМ, системы ЭВМ или их сети.

Ознакомление с компьютерной информацией посредством неправомерного к ней доступа может повлечь за собой возникновение отношения по возмещению причиненного вреда, если в его результате стала известна государственная, коммерческая или личная тайна. Модифицирование преступником информации о денежном балансе причиняет прямой материальный ущерб законному абоненту, так как с его лицевого счета снимаются денежные средства. При блокировании информации потенциально возможна ситуация упущенной выгоды. Например, законный владелец не сможет получить необходимую ему информацию, в результате чего потерпит убытки. Другим случаем может быть нарушение работы ЭВМ, которой для нормального функционирования ее программ необходим срочный регулярный выход в Интернет, нарушенный в результате блокирования доступа к нему. Копирование информации, например, может влечь отношения по неосновательному обогащению (сбережению). Уничтожение важных документов может также причинить серьезные убытки. Доказывание имущественного ущерба и убытков, с обоснованием их расчета, причиненных в результате преступления в сфере компьютерной информации, на практике представляется достаточно сложным и не всегда перспективным [8].

Доказывание сложных технических, программных и иных операций, входящих в специфику способа совершения преступления, доступным для суда языком достаточно проблематично [2]. Объяснение сути и последствий сложного преступления может быть затруднительно даже для высококвалифицированных специалистов и экспертов. Данные обстоятельства могут вызвать нежелание прокурора доказывать в суде отдельные эпизоды преступления или его состав целиком, если имеются предположения о проигрыше данного дела.

Особенности судебного разбирательства по делам о преступлениях в сфере компьютерной информации представляют большой интерес из-за слабой разработанности вопросов, связанных с применимостью и относимостью доказательств и сложностью, спецификой процесса доказывания. Их рассмотрение важно также в связи с неадаптированностью действующего уголовно-процессуального законодательства к появлению компьютерных преступлений и недостаточной аргументированностью и противоречивостью судебных решений.

Выявленные типичные черты неправомерного доступа к информации в сети Интернет являются общими и для преступлений, связанных с более опасными последствиями (в частности,

для жизни, здоровья, имущества), чем в рассмотренных случаях. Так, к наиболее важным общим элементам относится решающая роль завладения учетными записями владельцев. Значение имеет также использование информационной сети с удаленно расположенного компьютера, причем этот фактор, по нашему мнению, будет возрастать в связи с быстрым развитием телекоммуникационных систем связи. Эти обстоятельства необходимо учитывать при организации успешного противодействия преступлениям, связанным с неправомерным доступом к информации.

Рассмотренные в настоящей работе общие закономерности могут быть использованы для анализа преступлений в компьютерной сфере, предотвращения таких преступлений и организации профилактической работы, прежде всего с молодежью. Они могут также применяться при подготовке специалистов в учебных заведениях МВД и на юридических факультетах вузов.

Литература

1. Вехов В.Б. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие / В.Б. Вехов, В.В. Попова, Д.А. Илюшин. 2-е изд., доп. и испр. – М., 2004.

2. Гавло В.К. Некоторые аспекты разработки криминалистической характеристики компьютерных преступлений / В.К. Гавло, В.В. Поляков // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники: проблемы, тенденции, перспективы : тезисы докл. – М., 2005.

3. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. – М., 2005.

4. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук. – Воронеж, 2005.

5. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. – Воронеж, 2001.

6. Уголовное право Российской Федерации. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. – М., 2004 (Высшее образование).

7. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. А.А. Чекалин ; под ред. В.Т. Томина, В.С. Устинова, В.В. Сверчкова. – 2-е изд., испр. и доп. – М., 2004.

8. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх ; пер. с англ. – М., 1999.