Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 9, Is. 3, pp. 135-141, 2016

DOI: 10.13187/vesp.2016.9.135
www.ejournal21.com

Modern Security

UDC 004.056.53

The Criminal-Lawful and Criminological Characteristic of Incorrect Access to the Computer Information

Artem A. Gonchar [a, *], Xenia N. Zolotareva [b]

[a] St. Petersburg University of the Russian Interior Ministry, Russian Federation
[b] ITMO University, Russian Federation

Abstract

At present noticeably rises the degree of the risk of the loss of data, and also the possibility of their copying, modification, blocking. Moreover, this is not purely Russian, but world-wide tendency, in this case the perfection of computer technologies led to the appearance of new forms of crimes, in particular, to incorrect access to that guarded by the law of computer information. By its mechanism, using methods of accomplishment and concealment this crime has the specific character; it is characterized by the highest level of latency and by the low level of discoverability. This article examines some aspects of the criminal- lawful and criminological characteristic of incorrect access to the computer information.

Keywords: incorrect access to the computer information, crime in the sphere of computer information, the tracks of incorrect access to the computer information, article 272 UK RF.

1. Введение

В современных условиях научно-технического прогресса четко выделяется тенденция компьютеризации, создания разветвленных систем обработки данных, включающих в себя как мощные вычислительные комплексы, так и персональные компьютеры. Осуществляется ввод коммуникационных локальных, отраслевых, общегосударственных и межгосударственных сетей. Компьютеризация затрагивает практически все стороны общественной жизни от контроля за воздушным и наземным транспортом, до решения проблем национальной безопасности. Внедрение автоматизированных систем обработки информации способствует развитию экономики, приводит к появлению «безбумажных» технологий. Сейчас вряд ли кто может представить деятельность предприятия, организации, учреждения или фирмы, да и деятельность отдельных должностных лиц без использования компьютера (Черных, 1990).

Совершенствование компьютерных технологий привело к появлению новых видов преступлений, в частности, неправомерному доступу к охраняемой законом компьютерной

* Corresponding author
E-mail addresses: gonchar.tema@yandex.ru (A.A. Gonchar); ksenya2894@rambler.ru (X.N. Zolotareva)

информации. По своему механизму, способам совершения и сокрытия это преступление имеет определенную специфику, характеризуется высочайшим уровнем латентности и низким уровнем раскрываемости. Относительная новизна возникших проблем, стремительное наращивание процессов компьютеризации российского общества, рост компьютерной грамотности населения застали врасплох правоохранительные органы, оказавшиеся неготовыми к адекватному противостоянию и борьбе с этим новым экономико-социально-правовым явлением. Исследование сферы расследования неправомерного доступа к компьютерной информации является одной из немногих попыток на основе научного прогнозирования, обобщения зарубежного опыта, имеющейся в России следственной и судебной практики, дать рекомендации по расследованию нового вида преступлений (Шурухнов, 1999).

2. Материалы и методы

Методологической и теоретической основой исследования послужили положения материалистической диалектики как общенаучного метода познания, а так же системно-структурный, сравнительно-правовой, логический, исторический, статистический, контент-анализ, наблюдение, измерение, описание, сравнение и другие методы исследования. Правовой основой исследования явились законодательство Российской Федерации, указы Президента, нормативные акты Правительства и правоохранительных органов России.

3. Обсуждение

В России по данным ГИЦ МИД РФ в 1998 г. по ст. 272 УК РФ было возбуждено 55 уголовных дел, окончены расследованием 47. Это более чем в 10 раз превысило аналогичный показатель 1997 г. В 1999 году зарегистрировано 294 преступления, из них по ст. 272 – 209, по ст. 273 – 85. В 2000 году зарегистрировано 800 преступлений в сфере компьютерной информации. В 2003 году в России было возбуждено 1602 уголовных дела по ст. 272 («Неправомерный доступ к компьютерной информации») и 165 («Причинение имущественного ущерба путем обмана и злоупотребления доверием») УК РФ. Это составляет 76% от общего числа возбужденных уголовных дел по преступлениям в сфере компьютерной информации. Как следует из представленных данных, количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую, динамика роста которой составляет порядка 400 % ежегодно (Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам, 2015)). Прогнозирование ситуации показывает, что предстоящий рост неправомерного доступа к компьютерной информации будет объясняться следующими факторами:

1. Ростом количества ЭВМ, используемых в России, и как следствие этого, ростом количества их пользователей, увеличением объемов информации, хранимой в ЭВМ. Этому способствует снижение цен на сами компьютеры и периферийное оборудование (принтеры, сканеры, модемы и др.), а так же то обстоятельство, что отечественными фирмами налажена самостоятельная сборка компьютеров;
2. Недостаточностью мер по защите ЭВМ и их систем, а так же не всегда серьезным отношением руководителей к вопросу обеспечения информационной безопасности и защите информации;
3. Недостаточностью защиты программного обеспечения (к примеру, в системе Windows недостаточная защищенность программного обеспечения связана с несовершенным алгоритмом шифрования сохраняемых паролей);
4. Недостаточностью защиты самих технических средств защиты компьютерной техники;
5. Возможностью выхода российских пользователей ЭВМ в мировые информационные сети для обмена информацией, заключения контрактов, проведения платежей и др. Подобный обмен в настоящее время осуществляется абонентами самостоятельно, без контроля со стороны государственных органов, минуя географические и государственные границы;
6. Использованием в преступной деятельности современных технических средств, в том числе и ЭВМ. Это объясняется следующим: во-первых, организованная преступность

включена в крупномасштабный бизнес, выходящий за рамки отдельных государств, где без компьютеров невозможно руководить и организовывать сферу незаконной деятельности; во-вторых, из организаций, использующих электронно-вычислительную технику, значительно удобнее «вытягивать» деньги с помощью такой же техники, дающей возможность повысить прибыль и сократить риск;

7. Недостаточной защитой средств электронной почты;

8. Небрежностью в работе пользователей ЭВМ;

9. Непродуманной кадровой политикой в вопросах приема на работу и увольнения. Мировой опыт развития компьютерной техники свидетельствует, что специалисты высокой квалификации, неудовлетворенные условиями или оплатой труда, нередко уходят из компаний для того, чтобы начать собственный бизнес. При этом они «прихватывают» с собой различную информацию, являющуюся собственностью владельцев покидаемой фирмы, включая технологию, список потребителей и т.д.;

10. Низким уровнем специальной подготовки должностных лиц правоохранительных органов, в том числе и органов внутренних дел, которые должны предупреждать, раскрывать и расследовать неправомерный доступ к компьютерной информации;

11. Отсутствием скоординированности в работе государственных и общественных структур в сфере обеспечения информационной безопасности;

12. Ограничением на импорт в Россию защищенных от электронного шпионажа компьютеров и сетевого оборудования.

В этих условиях заметно повышается степень риска потери данных, а также возможность их копирования, модификации, блокирования. Причем, это не чисто российская, а общемировая тенденция. Представляется, что в скором времени проблема информационной безопасности и защиты данных станет в один ряд с такими глобальными проблемами современности, как межнациональные конфликты, экологический кризис, организованная преступность, отсталость развивающихся стран и др. (Ныркова, Каторин. Соколов, Ежгуров, 2013).

В связи с ростом анализируемых преступлений, возрастает количество тактических и методических ошибок, которые допускаются следователями и сотрудниками органов дознания, что объясняется, в первую очередь, отсутствием научно-обоснованных рекомендаций по расследованию неправомерного доступа к компьютерной информации. Наиболее распространенные способы несанкционированного доступа к компьютерной информации:

- доступ к информации во время отсутствия хозяина компьютера;
- элементарная кража компьютера со всем его содержимым;
- получение неправомерного доступа из внешней сети (локальной или глобальной) посредством взлома (Крылов, 1997).

Среди отечественных исследователей существует многообразие мнений о содержании признака неправомерности при доступе к компьютерной информации. Наиболее распространенное мнение заключается в том, что , неправомерным является доступ, при котором должны быть соблюдены два условия:

а) доступ к компьютерной информации является неправомерным, то есть нарушает нормативно-правовые и (или) локальные акты;

б) последствием такого доступа является уничтожение, блокирование, модификация либо копирование компьютерной информации.

Отсутствие согласия обладателя охраняемой законом компьютерной информации и нарушение порядка доступа к ней рассматривают в качестве признаков понятия «неправомерный доступ к компьютерной информации». Большинство правоведов полагает, что под неправомерным доступом следует считать самовольное получение виновным возможности распоряжаться такой информацией без согласия ее владельца или законного пользователя (Крылов, 1997).

В судебной практике определение неправомерности доступа, выработано следующим образом (Батурин, 1991):

- неправомерный доступ к компьютерной информации означает несанкционированный собственником информационной системы доступ к охраняемой законом компьютерной информации;

- неправомерным является доступ, осуществленный вопреки воле работодателей и без заключения договора с ними (Батурин, 1991).

4. Результаты

Способы совершения неправомерного доступа к компьютерной информации можно объединить в три основные группы:

Первая группа – это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а так же может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд непосредственно с того компьютера, на котором информация находится (Богумирский, 1994; Таили, 1997).

Вторая группа включает способы опосредованного (удаленного) доступа к компьютерной информации. К ним можно отнести: подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе; проникновение в чужие информационные сети, путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером; проникновение в компьютерную систему с использованием чужих паролей, выдавая при этом себя за законного пользователя (Богумирский, 1994; Таили, 1997).

К числу способов опосредованного (удаленного) доступа к компьютерной информации относятся способы непосредственного и электромагнитного перехвата. Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. Электромагнитный перехват компьютерный информации осуществляется за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. (Ныркова, Каторин. Соколов, Ежгуров, 2013).

Третью группу составляют смешанные способы, которые могут осуществляться как путем непосредственного, так и опосредованного (удаленного) доступа. К числу этих способов относятся: тайное введение в чужую программу таких команд, которые помогают ей осуществить новые, незапланированные функции при одновременном сохранении прежней ее работоспособности; модификация программ путем тайного встраивания в программу набора команд, которые должны сработать при определенных условиях, через какое-либо время; осуществление доступа к базам данных и файлам законного пользователя путем нахождения слабых мест в системах защиты (Сергеев, 1997).

Неправомерный доступ к компьютерной информации может быть связан и с насилием над личностью либо угрозой его применения (Ляпунов, Максимов, 1997).

Способы сокрытия рассматриваемого преступления в значительной степени детерминированы способами его совершения. При непосредственном доступе к компьютерной информации, сокрытие следов преступления сводится к воссозданию обстановки, предшествующей совершению преступления, т.е. уничтожению оставленных следов (следов пальцев рук, следов обуви, микрочастиц и пр.). При опосредованном (удаленном) доступе сокрытие заключается в самом способе совершения преступления, который затрудняет обнаружение неправомерного доступа. Это достигается применением чужих паролей, идентификационных средств доступа и т.д. (Ляпунов, Максимов, 1997).

Одним из распространенных орудий неправомерного доступа к компьютерной информации является сам компьютер. Необходимо различать орудия непосредственного и опосредованного доступа. К орудиям непосредственного доступа можно отнести, прежде всего, машинные носители информации, а так же все средства преодоления защиты информации.

К орудиям опосредованного (удаленного) доступа относится, прежде всего, сетевое оборудование (при неправомерном доступе из локальных сетей), а так же средства доступа в удаленные сети (средства телефонной связи, модем) (Ветров, Ляпунов, 1997).

Другим распространенным средством совершения неправомерного доступа в последнее время стала глобальная мировая телекоммуникационная среда Интернет (Букин, 1997).

Одним из распространенных орудий неправомерного доступа к компьютерной информации является сам компьютер.

Обстановку совершения неправомерного доступа к компьютерной информации составляют обстоятельства, характеризующие вещественные, технические, пространственные, временные, социально-психологические особенности события рассматриваемого преступления.

Особенностью данного преступления является то, что на него практически не оказывают влияние природно-климатические факторы. Дополнительными факторами, характеризующими обстановку совершения неправомерного доступа к компьютерной информации могут являться наличие и состояние средств защиты компьютерной техники (организационных, технических, программных), сложившаяся на объекте дисциплина, требовательность со стороны руководителей по соблюдению норм и правил информационной безопасности и эксплуатации ЭВМ. Для обстановки, в которой возможно совершение рассматриваемого преступления, наиболее свойственно следующее: невысокий технико-организационный уровень хозяйственной деятельности и контроль над информационной безопасностью, не налаженная система защиты информации, атмосфера безразличия к случаям нарушения требований информационной безопасности. Так же особенностью неправомерного доступа к компьютерной информации является то, что место непосредственного совершения противоправного деяния – (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать. Причем это имеет место практически при каждом случае опосредованного (удаленного) доступа к компьютерной информации (Букин, 1997).

Следы неправомерного доступа к компьютерной информации подразделяются на два вида: традиционные следы, рассматриваемые трасологией, и нетрадиционные - информационные следы.

К первому типу относятся материальные следы. Ими могут быть рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т.д.), а так же на магнитных носителях и CD-ROM дисках. (Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам, 2015; Букин, 1997).

Информационные следы образуются в результате воздействия (уничтожения, модификации, копирования, блокирования) на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Прежде всего, они остаются на магнитных носителях информации и отражают изменения в хранящейся в них информации (по сравнению с исходным состоянием). Речь идет о следах модификации информации (баз данных, программ, текстовых файлов), находящейся на жестких дисках ЭВМ, дискетах, магнитных лентах, лазерных и магнито-оптических дисках. Кроме того, магнитные носители могут нести следы уничтожения или модификации информации (удаление из каталогов имен файлов, стирание или добавление отдельных записей, физическое разрушение или размагничивание носителей). Информационными следами являются так же результаты работы антивирусных и тестовых программ. Данные следы могут быть выявлены при изучении компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, а так же программного обеспечения. Для выявления подобных следов необходимо участие специалистов в сфере программного обеспечения и вычислительной техники (Букин, 1997).

Способы сокрытия рассматриваемого преступления в значительной степени детерминированы способами его совершения. При непосредственном доступе к компьютерной информации сокрытие следов преступления сводится к воссозданию обстановки, предшествующей совершению преступления, то есть, уничтожению оставленных следов (следов пальцев рук, следов обуви, микрочастиц и пр.). При опосредованном (удаленном) доступе сокрытие заключается в самом способе совершения преступления, который затрудняет обнаружение неправомерного доступа. Это достигается применением чужих паролей, идентификационных средств доступа и т. д. (Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам, 2015).

5. Заключение

Совершенствование компьютерных технологий привело к появлению новых видов преступлений, в частности, неправомерному доступу к охраняемой законом компьютерной информации. По своему механизму, способам совершения и сокрытия это преступление имеет определенную специфику, характеризуется высочайшим уровнем латентности и низким уровнем раскрываемости (Крылов, 1997).

Совершенно необязательно обладать какой-либо важной и сверхсекретной компьютерной информацией, чтобы стать жертвой компьютерного преступника. Взломать ваш компьютер и отформатировать вам жесткий диск со всеми данными могут и просто из хулиганских побуждений (Букин, 1997).

Неправомерный доступ к компьютерной информации необходимо отличать от преступления, предусмотренного ст. 274 УК РФ. Указанная статья устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации (Ветров, Ляпунов, 1997).

Под доступом к компьютерной информации следует понимать получение возможности обращения к компьютерной информации, в результате которого лицо получает правомочия обладателя информации. Признаками неправомерного доступа к компьютерной информации, является отсутствие соответствующего разрешения со стороны обладателя. Несанкционированный доступ опасен не только прочтением личной информации, но и возможностью постороннего контроля над системой с помощью управляемых программных закладок.

Не вызывает сомнений тот факт, что для более серьезной защиты компьютера встроенных средств операционной системы недостаточно. Поэтому наряду со стандартными средствами защиты не помешает использовать специальные средства. Их делят на два вида: средства, ограничивающие физический доступ, и средства, ограничивающие доступ по сети. Наиболее надежное решение этой проблемы – использование аппаратных средств защиты, начинающих работу до загрузки операционной системы компьютера. Такие средства защиты называются «электронными замками». На подготовительном этапе использования выполните установку и настройку замка. Обычно настройка выполняется администратором по безопасности (Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам , 2015).

Примечания

Батурин, 1991 - *Батурин Ю.М.* Проблемы компьютерного права. М.: Юрид. лит., 1991.

Богумирский, 1994 - *Богумирский Б.С.* Руководство пользователя ПЭВМ. СПб., 1994.

Букин, 1997 - *Букин Д.* Хакеры. О тех, кто делает это // *Рынок ценных бумаг*, 1997. № 23, с. 54—57.

Ветров, Ляпунов, 1997 - *Ветров Н.И., Ляпунов Ю.И.* Уголовное право. Общая часть: Учебник. М.: Новый Юрист, КноРус. 1997.

Крылов, 1997 - *Крылов В.В.* Информационные компьютерные преступления. М., 1997.

Ляпунов, Максимов, 1997 - *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // *Законность*, 1997. № 1.

Нырков и др., 2013 - *Нырков А.П., Каторин Ю.Ф., Соколов С.С., Ежгуров В.Н.* Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. // *Проблемы информационной безопасности. Компьютерные системы*, 2013. № 2 (2), с. 54-58.

Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам, 2015 - *Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам*. М.: Спарк. 2015.

Сергеев, 1997 - *Сергеев В.В.* Компьютерные преступления в банковской сфере // *Банковское дело*, 1997. № 2.

Таили, 1997 - *Таили Э.* Безопасность компьютера. Минск, 1997.

Черных, 1990 - *Черных А.В.* Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) // *Советское государство и право*, 1990. №6.

Шурухнов, 1999 – *Шурухнов Н.Г.* Расследование неправомерного доступа к компьютерной информации. Научно-практическое пособие. М., 1990.

References

Baturin, 1991 - *Baturin Yu.M.* (1991). Problemy komp'yuternogo prava. M.: Yurid. lit.

Bogumirskii, 1994 - *Bogumirskii B.S.* (1994). Rukovodstvo pol'zovatelya PEVM. SPb.

Bukin, 1997 - *Bukin D.* (1997). Khakery. O tekh, kto delaet eto // Rynok tsennykh bumag, № 23, s. 54—57.

Vetrov, Lyapunov, 1997 - *Vetrov N.I., Lyapunov Yu.I.* (1997). Ugolovnoe pravo. Obshchaya chast': Uchebnik. M.: Novyi Yurist, KnoRus.

Krylov, 1997 - *Krylov V.V.* (1997). Informatsionnye komp'yuternye prestupleniya. M.

Lyapunov, Maksimov, 1997 - *Lyapunov Yu., Maksimov V.* (1997). Otvetstvennost' za komp'yuternye prestupleniya // Zakonnost', № 1.

Nyrkov, Katorin. Sokolov, Ezhgurov, 2013 - *Nyrkov A.P., Katorin Yu.F., Sokolov S.S., Ezhgurov V.N.* (2013). Osnovnye printsipy postroeniya zashchishchennykh informatsionnykh sistem avtomatizirovannogo upravleniya transportno-logicheskim kompleksom. //Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy, № 2 (2), s. 54-58.

Sbornik postanovlenii Plenumov Verkhovnykh Sudov SSSR i RSFSR (Rossiiskoi Federatsii) po ugolovnym delam , 2015 - *Sbornik postanovlenii Plenumov Verkhovnykh Sudov SSSR i RSFSR (Rossiiskoi Federatsii) po ugolovnym delam* (2015). M.: Spark.

Sergeev, 1997 - *Sergeev V.V.* (1997). Komp'yuternye prestupleniya v bankovskoi sfere // Bankovskoe delo, № 2.

Taili, 1997 -*Taili E.* (1997). Bezopasnost' komp'yutera. Minsk.

Chernykh, 1990 - *Chernykh A.V.* (1990). Obespechenie bezopasnosti avtomatizirovannykh informatsionnykh sistem (ugolovno-pravovye aspekty) // *Sovetskoe gosudarstvo i pravo*, №6.

Shurukhnov, 1999 – *Shurukhnov N.G.* (1990). Rassledovanie nepravomernogo dostupa k komp'yuternoi informatsii. Nauchno-prakticheskoe posobie. M.

УДК 004.056.53

Уголовно-правовая и криминалистическая характеристика неправомерного доступа к компьютерной информации

А.А. Гончар [a, *], К.Н. Золотарева [b]

[a] Санкт-Петербургский Университет МВД России, Российская Федерация
[б] Университет ИТМО, Российская Федерация

Аннотация. В настоящее время заметно повышается степень риска потери данных, а также возможность их копирования, модификации, блокирования. Причем, это не чисто российская, а общемировая тенденция, при этом совершенствование компьютерных технологий привело к появлению новых видов преступлений, в частности, неправомерному доступу к охраняемой законом компьютерной информации. По своему механизму, способам совершения и сокрытия это преступление имеет определенную специфику, характеризуется высочайшим уровнем латентности и низким уровнем раскрываемости. В данной статье рассмотрены некоторые аспекты уголовно-правовой и криминалистической характеристики неправомерного доступа к компьютерной информации.

Ключевые слова: неправомерный доступ к компьютерной информации, преступление в сфере компьютерной информации, следы неправомерного доступа к компьютерной информации, статья 272 УК РФ.

* Корреспондирующий автор
E-mail addresses: gonchar.tema@yandex.ru (А.А. Гончар); ksenya2894@rambler.ru (К.Н. Золотарева)