



УДК 004.7

**КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ:
СУЩНОСТЬ, ОСОБЕННОСТИ И ВОЗМОЖНОСТИ ПРЕДОТВРАЩЕНИЯ**
**COMPUTER CRIME: THE NATURE, CHARACTERISTICS AND POSSIBLE
PREVENTION**

С.В. Минаев
S.V. Minaev

Орловский Государственный Университет имени И.С. Тургенева
Россия, 302026, г. Орёл, ул. Комсомольская, д. 95

Orel State University named after I.S. Turgenev, 95 Komsomolskaya St, Orel, 302026, Russia

E-mail: gam-gam16@mail.ru

Аннотация

В данной статье раскрывается понятие компьютерной преступности, а также её цели и мотивы. Дается анализ мер контроля над компьютерной преступностью и повествуется о направлениях повышения эффективности контроля над компьютерной преступностью в России.

Abstract

This article deals with the concept of computer-related crime, as well as its goals and motives. Also analyzed measures to control computer-related crime, and tells the story of directions of increase of efficiency of control over the computer crime in Russia.

Ключевые слова: вычислительная машина, преступление, контроль, мыслительная деятельность, информация.

Keywords: computer, crime, control, intellectual activity, information.

Понятие "компьютерная преступность" впервые было использовано в американской, а затем и в другой зарубежной печати в начале 60-х годов. Компьютерное преступление - это любого рода незаконное или неразрешенное поведение, которое воздействует на автоматизированную обработку данных и (или) передачу данных[4].

О данном феномене свидетельствует большой перечень всевозможных вариаций компьютерных преступлений. Объектами такого рода посягательств могут быть, не только технические средства (компьютеры и периферия), но и материальные объекты, в том числе базы данных и программное обеспечение.

Первый случай злоупотребления при помощи компьютера зарегистрирован ещё в 1958 году, а первое преступление с использованием компьютера было совершено в 1979 году в Вильнюсе.[1]

Существует множество определений понятия «компьютерное преступление».

Компьютерные преступления - это действия, совершаемые с целью получения и использования информации в компьютерной сфере. А компьютерная информация может быть, как предметом, так и средством совершения преступления.[2. с. 11]

К «компьютерным преступлениям» относятся любого рода преступления, связанные с компьютерной техникой, которые при этом противоречат праву.[3. с. 20]

По мнению Бекряшева А. К. под компьютерным преступлением следует считать незаконное и неразрешенное поведение, которое тесно соприкасается с обработкой и передачей данных.[4. с.12]



Под компьютерными преступлениями выделяют опасные действия, предусмотренные уголовным законом, в которых информация ЭВМ является объектом преступления.[5, с. 17]

После долгих и достаточно продолжительных исследований данного феномена был выдвинут ряд основных подходов к определению понятия компьютерной преступности.

В уголовно-правовой сфере под компьютерным преступлением понимают нарушения личных интересов и чужих прав в отношении любого вида автоматизированных систем обработки данных, которые намеренно совершаются во вред правам и интересам людей, общества и государства. Всё это предусмотрено и карается по всей строгости уголовного закона.[15]

Как предполагают многие отечественные и зарубежные специалисты, следует выделить два главных точки зрения научной мысли по данному вопросу. Белозеров И.П. и Копырюлин, А.Н. к компьютерным преступлениям относят преступления, где непосредственно ЭВМ является, как орудием для покушения на чью-то информацию, так и объектом, с целью получения выгоды и нанесению ущерба другой стороне. А хищение ЭВМ само собой рассматривается как один из путей осуществления преступлений в компьютерной среде.

Батурин Ю.М. и Жодзишский А.М. относят к компьютерным преступлениям только действия в сфере автоматизированной обработки информации, направленные против закона.[6, с. 112]

В XXI веке компьютерная преступность стала одним из самых опасных и уязвимых видов преступных деяний, которые непосредственно касаются жизни людей и их имущества. Из-за постоянного развития технических средств, при помощи которых можно проникать во все без исключения сферы деятельности общества, постоянно усугубляются проблемы информационной безопасности человека.

В современной науке принято выделять несколько видов компьютерной преступности:

- Незаконный доступ к компьютерной информации.
- Осуществление различных операций путём создания вредоносных программ для ЭВМ.
- Неправильная эксплуатация ЭВМ.

Незаконный доступ к компьютерной информации. Данный вид компьютерной преступности подразумевает проникновение к чужой информации, путём взлома паролей и краж различных информационных носителей. Эти действия наносят вред, как для интересов собственника, так и для самой информации, которую злоумышленник может уничтожить, продать, видоизменить или же заблокировать, тем самым используя её в корыстных целях. [7, с.14]

А.Н. Копырюлин отмечал, что противоправным доступом также нужно считать и посещение ресурсов сети Интернет без устного или письменного разрешения хозяина, при которой данная информация будет подвержена всевозможным изменениям.[8, с.21]

Следует сказать, что этот вид компьютерной преступности в основном совершается для кражи информации, с целью получения выгоды. Преступники из года в год совершенствуют свои навыки, модифицируя программное обеспечение, создают всевозможные программы, при помощи которых оборот в финансовом эквиваленте преумножается в разы.

Осуществление различных операций путём создания вредоносных программ для ЭВМ. Данный вид компьютерной преступности является самым распространённым в сети. Вредоносные программы позволяют прервать оптимальную работу ЭВМ. Объектами для данного противоправного деяния являются ЭВМ и их программные обеспечения, у которых изменяется информационное содержание.



Само создание любой вредоносной программы подразумевает создание антивируса. Многие крупнейшие корпорации за счёт этого заработали немалые состояния, которые в дальнейшем вкладывались в модернизацию новейших версий своих программ.

А что касается относительно мелких (как по финансовым вложениям, так и по масштабам ущерба) вредоносных программ, то они могут, через созданный и запрограммированный код, в любое мгновение взломать и нарушить работу системы нужной ЭВМ.

По мнению Маслаковой Е., вредоносные программы, такие как: «черви», «трояны», вирусы программного обеспечения в сети Интернет имеют достаточно большую популярность. Но при этом некоторые программы, как только выходят из-под контроля своих создателей, они могут самопроизвольно нанести ощутимый вред.[9]

Наиболее важную нишу среди программ, способных наносить вред, занимают компьютерные вирусы, которые могут распространяться сами по себе путём запуска определённого кода.[10, с.29]

Неправильная эксплуатация ЭВМ. Для любого современного человека выход из строя компьютера может привести к определённым последствиям негативного характера. Посему должен быть создан свод определённых правил в плане эксплуатации ЭВМ, для того, чтобы компьютерное оборудование было целым и невредимым, а сохранность информации была на недостижимом для преступников уровне. Если же в отношении информации происходит нечто негативное, приносящее моральный и физический вред владельцу, то данные деяния караются законом.[11, с.3]

Правила эксплуатации ЭВМ определены и закреплены различными нормативно-правовыми актами. Данные правила могут быть установлены, как уполномоченным государственным органом, так и могут быть приняты в организации в виде нормативных правил внутреннего распорядка.

Именно поэтому нарушение и неповиновение данным нормам касается только технических правил, но не форм работы ЭВМ или их закреплённой регламентации.[2, с.58]

Что касается размера нанесённого вреда, то он оценивается путём установления характера вреда здоровью, материальный ущерб, восстановление и нормализация деятельности ЭВМ и потерянной или же повреждённой информации.[7]

Батурин Ю.М. считает, что неправильная эксплуатация ЭВМ в любом случае подразумевает умышленную форму вины. Причастный к преступлению заранее осознаёт, что нарушает работу ЭВМ, нанося существенный вред, охраняемой законом информации и причиняет вред, думая только лишь о себе, а к остальным его отношение безразлично. [12, с.46]

Что касается криминологических групп компьютерных преступлений, то их принято разделять на:

- компьютерные преступления в экономической сфере,
- компьютерные преступления, затрагивающие личные права и неприкосновенность частной сферы,
- компьютерные преступления против интересов общества и государства.

К основным целям совершения преступлений в сфере компьютеров принято относить следующие:

- подделка платежных ведомостей и финансовых отчетов,
- фальсификация документов с целью получения незаконной прибыли;
- перечисление и обналичивание финансовых средств на подставных лиц.[13]

Среди основных мотивов, побуждающих пойти на деяние в сфере компьютерных преступлений, принято выделять:

- выплата долгов, а также выход из продолжительной финансовой ямы;
- доказательство своего превосходства над искусственным интеллектом;
- получение статуса «звезды», о котором будут знать все через СМИ.[7]

Особой сложностью данных преступлений являются: чрезвычайно большая скрытность, сбор тщательных доказательств, транснациональный характер (чаще всего, с ис-



пользованием телекоммуникационных систем), оценка нанесённого материального ущерба, а также специфичность и индивидуальный почерк самих преступников. Как правило, в большинстве своём, ими являются служащие банка (как действующие, так и ранее уволенные), которые осведомлены об информационной безопасности. Также среди такого рода преступников очень часто встречаются высококвалифицированные программисты, способные идти против закона и при этом оставаясь безнаказанными.

Чаще всего преступления в компьютерной сфере совершаются в банковской сфере, которая непосредственно связана с финансами. Но чрезвычайно большая скрытность таких компьютерных преступлений обусловлена тем, что многие пострадавшие фирмы и кампании стараются разрешить данную ситуацию только своими силами.[4]. Директора и руководители потерпевших компаний больше всего боятся и опасаются подрыва репутации, что способствует огромному минусу для их бизнеса.

Лиц, совершивших компьютерные преступления, можно объединить в несколько обширных групп:

- лица, которые имеют определённые связи с жертвой, но при этом не работающие в данной организации;
- непосредственно сотрудники организации, занимающие ответственные посты и имеющие особый доступ к защищённой информации;
- сотрудники, работающие за компьютерами, и при этом злоупотребляющие своим положением и доверием.[17]

Специалисты из США, а в частности Крис Викери, подразделяют носящий вред персонал на категории в соответствии со сферами деятельности:

- Операционные преступления, совершающиеся только операторами ЭВМ и обслуживающими линии телекоммуникации.
- Преступления, основанные на использовании программного обеспечения, обычно совершаются лицами, которые имеют к ним прямой доступ.
- Для аппаратурной части компьютерных систем опасность совершения преступлений представляют инженеры по различным устройствам.[14]

Можно сделать достаточно простой, но при этом смелый вывод, что любой из работников таит в себе определённую опасность и при любом удобном случае он может воспользоваться ситуацией и начать действовать.

Например, по сведениям Национального центра данных о преступности, связанной с ЭВМ (Лос-Анджелес, США), около 85% злоупотреблений в сфере финансов, связанных с нарушениями в области информационной безопасности, случается при содействии (как прямом, так и косвенном) работников банка. При этом на преступный путь чаще всего, как ни странно, становятся самые видные и более высококлассные сотрудники, обладающие максимальными правами в компьютерных системах компании.[13]

В зависимости от способа воздействия на компьютерную систему специалисты выделяют несколько видов компьютерных преступлений:

- Физические злоупотребления, которые включают в себя деструкцию оборудования, как частичное повреждение, так и полное уничтожение ценных информации.
- Операционные злоупотребления, чаще всего: подмена носителей и считывающих устройств, выдача себя за другое лицо путём мошенничества.
- Программные злоупотребления, из-за которых может измениться работа всей системы, но данную неполадку можно будет обнаружить только спустя определённое время.[16]

Границы управления над преступностью в компьютерной сфере подразделяются на организационно-тактические, правовые и программно-технические.

К организационно-тактическим мерам относятся: круглосуточная охрана вычислительных центров, особая тщательность при приёме на работу персонала и т.п.

К правовым мерам относятся разработка особых правил, устанавливающих ответственность за совершение компьютерных преступлений, в том числе постоянная защита



авторских прав программистов, а также вопросы контроля за разработчиками компьютерных систем.

По мнению Бачило И. Д., к программно-техническим мерам можно отнести защиту от несанкционированного взлома центральной системы, профилактику от множества вредоносных компьютерных вирусов, создание и хранение особо важных копий ценных документов, установку резервных систем бесперебойного электропитания и другие меры безопасности.[18]

Главной целью государственной политики в сфере компьютерных преступлений является создание единой мощной национальной системы борьбы с преступлениями в сфере информации.

Борьба с компьютерной преступностью в России осуществляется в условиях действия комплекса факторов, снижающих ее эффективность. К наиболее значимым относятся[19]:

- отсутствие эффективной системы обеспечения законных интересов граждан и общества в сфере информационной безопасности;
- недостаточное финансирование по улучшению базы информационной безопасности;
- слабость координации действий по борьбе с компьютерными преступлениями.

К основным направлениям повышения эффективности контроля над компьютерной преступностью в РФ следует выделить[18]:

- формирование целостной системы постоянного мониторинга обстановки в сфере обеспечения информационной безопасности и своевременное пресечение компьютерных преступлений;
- организация взаимодействия и координация усилий различных правоохранительных органов друг с другом;
- сотрудничество и тесное взаимодействие правоохранительных органов РФ и зарубежных стран по борьбе с преступлениями в сфере компьютеров;

Помимо создания такой системы, важен вопрос по кадрам. Если система не будет иметь в своих рядах самых квалифицированных работников, то её эффективность не будет столь высока, как хотелось бы. Со стороны государства важно сделать своего рода «перегрузку» в данной сфере. Нужно перенять ценный опыт от других зарубежных стран, выстроить особую систему обучения для специалистов, которые будут вести борьбу с компьютерными преступлениями.

Но при этом хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения никогда не смогут дать стопроцентные гарантии на абсолютную надежность и безопасность данных в компьютерных сетях. Но в то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности, не забывая об осторожности.[20]

Можно с уверенностью сказать, что на сегодняшний день уголовное законодательство в сфере компьютерной информации, мягко говоря, не идеально. Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов компьютерных посягательств, которые совершаются на сегодняшний день. И требуют серьезных работ.

Таким образом, компьютерные преступления в обозримом будущем будут и далее совершенствоваться. Но для того, чтобы процент данных преступлений значительно снизился, государство должно занимать не выжидательную позицию, а конкретно действовать и оберегать своих граждан.

Список литературы References

1. 1994-1998 Энциклопедия Britannica.
1994-1998 Encyclopedia Britannica.



2. Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы [Москва: Майор (Осипенко), 2001 – 190 с.].
Leontiev B. K. Hackers, crackers, and other information the killer [Moscow: Major (Osipenko), 2001 - 190 s.].
3. Седаков С.Ю., Филиппова Т. П. Хрестоматия по всеобщей истории государства и права [М.: Юрист, 1996. - 391 с.].
Sedakov S.Y., Filippova T. P. Readings on the general history of the state and law [M.: Lawyer, 1996. - 391 s.].
4. Бекряшев А. К., Белозеров И. П. Теневая экономика и экономическая преступность [2003].
Bekryashev A. K., Belozеров I. P. Shadow Economy and Economic Crime [2003].
5. Вехов В. Б. Уголовный кодекс Российской Федерации: постатейный комментарий [Указ. Соч.].
Vekhov V. B. The Criminal Code of the Russian Federation: Commentaries [Decree. Cit.].
6. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность [Юридическая литература, Москва, 1991 – 159 с.].
Baturin J. M. The computer crime and computer security [Legal Literature, Moscow, 1991 - 159 s.].
7. Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты [Тамбов, автореф. дис, 2007].
Koryulyin A. N. The crimes in the sphere of computer information: criminally-legal and criminological aspects of the [Tambov, Cand. Thesis, 2007].
8. Копырюлин А. Н. Квалификация преступлений в сфере компьютерной информации [Законность. – 2007].
Koryulyin A. N. Qualification of crimes in the sphere of computer information [Act. - 2007].
9. Маслакова Е. Вредоносные программы для ЭВМ в глобальных компьютерных сетях [Юридический мир. – 2005. – № 11 // СПС КонсультантПлюс. – 2007].
Maslakova E. Malicious computer program on a global computer network [Legal World. - 2005. - № 11 // SPS Consultant. - 2007].
10. Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений [М.: Собрание, 2004].
Soloviev L. N. Malicious programs: investigation and prevention of crimes [M.: Collection, 2004].
11. Попова А. В. Автоматизированные системы управления [Минск, 2006 – 352 с.].
Popova A. V. The automated control systems [Minsk, 2006 - 352 pp.].
12. Полевой Н. С. Правовая информатика и кибернетика [Учебник, М: Юрид. лит., 1993].
Polevoy N. S. Legal Informatics and Cybernetics [Tutorial, M: jurid. Lighted 1993].
13. Здравомыслов Б. В. Уголовное право России. Особенная часть: Учебник, М.: Юрист, 1996.
Zdravomyslov B. V. Criminal Law of Russia. Special part: Textbook, M.: Lawyer, 1996.
14. Борьба с компьютерной преступностью за рубежом (на примере США, Великобритании, Франции, Польши): Обзорная информация. Зарубежный опыт. Вып.14. – М.: ГИЦ МВД РФ, 2003.
The fight against computer crime abroad (in the example of the USA, the UK, France, Poland): Overview. Foreign experience. Вып.14. - М.: GIZ Ministry of Internal Affairs of the Russian Federation, 2003.
15. Анин Б. Защита компьютерной информации. – СПб.: BHV, 2000.
Anin B. Protection of computer information. - SPb.: BHV, 2000.
16. Батурин Ю. М. Проблемы компьютерного права. - М.: Юриздат, 1991.
Baturin Y. M. Problems of computer law. - M.: Yurizdat 1991.
17. Сударева Л. А. Личность преступника, совершившего компьютерные преступления // Вестник Московского университета МВД. – 2007. – № 1.
Sudareva L. A. identity of the perpetrator who committed computer crimes // Bulletin of Moscow University of the Interior Ministry. - 2007. - № 1.
18. Бачило И. Д. Компьютерная преступность: особенности и методы борьбы // Современное право. – 2006. – № 4.
Bachilo I. D. Computer crime: the features and control methods // Modern Law. - 2006. - № 4.
19. Минаев В. А., Саблин В. Н. Основные проблемы борьбы с компьютерными преступлениями в России. Экономика и производство. Компьютерный ресурс.
Minaev V. A Sablin V. N. The main problems of the fight against computer crime in Russia. Economy and production. Computer resource.
20. Вехов В. Б. Компьютерные преступления: Способы совершения. Методики раскрытия [М.: Право и Закон, 1996].
Vekhov V.B. Computer crime: How the commission. Methods of disclosure [M.: Law and the Law of 1996].