УДК 343.34

Д. Л. Никишин
Институт Академии ФСИН России, Рязань

Д. О. Орешкова
Академия ФСИН России, Рязань, e-mail: fuf62@mail.ru

КРАТКИЙ АНАЛИТИЧЕСКИЙ АНАЛИЗ УГОЛОВНО-ПРАВОВОЙ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ключевые слова: информационные технологии, киберпреступность, Интернет-ресурсы, меры предупреждения компьютерных преступлений, уголовно-правовая борьба с преступлениями в сфере информационных технологий, личность преступника.

Статья посвящена актуальным проблемам преступлений в сфере компьютерной информации. В частности, авторы научной статьи рассматривают основные аспекты преступлений данного вида. В статье анализируется сущность компьютерной преступности, ее причины, условия зарождения и дальнейшего «развития». Авторы статьи называют и характеризуют основные группы мер предупреждения компьютерных преступлений, к которым, в частности, можно отнести: правовые, организационно-технические и криминологические меры. Отмечается, что профилактика и предупреждение любых, в том числе и компьютерных преступлений, должна носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих структур. Проанализировав материалы ряда уголовных дел, а также статистические данные, авторы статьи предлагают примерное описание портрета личности преступника, совершившего преступление в сфере информационных технологий: дается описание его характера, социального положения, умственных способностей, рассматривают возрастные, половые, социальные и нравственные особенности преступников. Авторами делается вывод о том, что современные уголовно-правовые способы борьбы с компьютерными преступлениями, несомненно, нуждаются в дальнейшем изучении, которое позволит выявить важнейшие проблемные аспекты и вопросы, что позволит найти наиболее верные пути их решения.

D. L. Nikishin
Institute of the Academy of Law Management of the Federal Penitentiary Service of Russia, Ryazan

D. O. Oreshkova
The Academy of Law Management of the Federal Penitentiary Service of Russia, Ryazan, e-mail: fuf62@mail.ru

SHORT ANALYTICAL ANALYSIS OF THE CRIMINAL LAW FIGHT AGAINST CRIMES IN THE FIELD OF COMPUTER INFORMATION

Keywords: information technology, cybercrime, Internet resources, measures to prevent computer crimes, criminal law fight against crimes in the field of information technology, identity of the perpetrator.

The article is devoted to topical problems of crimes in the field of computer information. In particular, the authors of the scientific article consider the main aspects of this type of crime. The article analyzes the essence of computer crime, its causes, conditions of origin and further "development". The authors of the article name and characterize the main groups of measures to prevent computer crimes, which, in particular, include: legal, organizational, technical and criminological measures. It is noted that the prevention and prevention of any crime, including computer crimes, should be comprehensive and fall under the competence of state bodies, and not various commercial structures. After analyzing the materials of a number of criminal cases, as well as statistical data, the authors of the article offer an approximate description of the personality portrait of a criminal who committed a crime in the field of information technology: a description of his character, social status, mental abilities is given, and the age, sex, social and moral characteristics of criminals are considered. The authors conclude that modern criminal law methods of combating computer crimes undoubtedly need further study, which will reveal the most important problematic aspects and issues, which will allow finding the most correct ways to solve them.

На сегодняшний день одним из наиболее актуальных направлений политики государства является борьба с таким видом преступлений, как преступления в сфере компьютерной информации. В первую очередь, это обусловлено тем, что с каждым днем жизнь людей все больше и больше начинает зависеть от IT-технологий. Ежедневно люди пользуются Интернет-ресурсами, заходят в различные социальные сети; работа большинства специалистов связана именно с информационными технологиями… [1]

С ростом значимости компьютерных технологий в жизни общества наблюдается постепенное увеличение числа правонарушений в данной сфере.

Следует отметить, что стремительное нарастание информационных разработок, внедрение достижений науки и технического прогресса во все сферы общества обуславливают не только коренные прогрессивные изменения в составе факторов экономического развития России, но и порождают негативные тенденции развития преступного мира, приводят к появлению новых форм и видов преступных посягательств. Это может проявляться, например, в том, что преступники зачастую в своей деятельности прибегают к новейшим достижениям компьютеризации.

Важнейшим (и в то же время тревожнейшим) последствием этого становится зарождение и развитие в России нового вида преступных посягательств, которые ранее не были известны отечественной юридической науке и судебной практике, – преступлений, связанных с использованием средств компьютерной техники и информационно-обрабатывающих технологий, т.е. компьютерных преступлений.

Целью данного исследования является изучение особенностей преступлений в сфере компьютерной информации и нахождение возможных путей предупреждения таких преступлений. Методологическую основу исследования составляют общенаучные и частно-научные (историко-правовой, статистический) методы познания.

Рассматриваемые преступления нашли свое отражение в главе 28 УК РФ – «Преступления в сфере компьютерной информации». К ним относятся:

– неправомерный доступ к компьютерной информации (статья 272 УК РФ);

– создание, использование и распространение вредоносных программ (статья 273 УК РФ);

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ);

– неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ).

В настоящее время с развитием всех сфер общества в эпоху глобальной информатизации компьютерная преступность стала реальностью.

Государственное обеспечение безопасности общества от компьютерной преступности заключается в принятии *правовых* (направленных на формирование современного законодательства, призванного регулировать указанные правонарушения, а также устанавливающего адекватную уголовную и другие виды ответственности) и *организационных* (создание надежной материально-технической базы и подготовку высококвалифицированных специалистов) мер.

В сложившейся ситуации необходимо точечно изучить и проанализировать сущность компьютерной преступности, причины и условия ее зарождения и дальнейшего «развития».

Понятие «компьютерная преступность» впервые было зафиксировано в начале 60-х годов в американских источниках. Компьютерная информация является предметом и (или) средством совершения преступления. Другими словами, компьютерная преступность – это особый вид преступлений, который связан с незаконным использованием современных информационных технологий и средств компьютерной техники.

Информационные технологии (ИТ) как важнейшая область науки и техники оказывают значительное влияние на все сферы общества, в какой-то степени ограничивают затраты труда людей и природных ресурсов, благотворно влияют на образовательную, социально-культурную деятельность человека [2].

В соответствии с определением, принятым ЮНЕСКО, под информационными технологиями следует понимать совокупность связанных между собой дисциплин научного, технологического, инженерного характера, которые изучают:

– методы эффективной организации труда людей, работающих в сфере информационных технологий;

– вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием;

– связанные с этим социальные, экономические и культурные проблемы и аспекты.

Информация становится продуктом общественных (информационных) отношений, начинает приобретать товарные черты и становится продуктом купли-продажи. В результате чего возникают и формируются новые социальные отношения. На сегодняшний день можно констатировать значительный объем договорных отношений, связанных с изготовление, передачей, накоплением и использованием информации в самых различных её формах: научно-технической документации, программного обеспечения ЭВТ, баз данных, систем управления базами данных (СУБД) и т.д. [3].

Криминологически значимы следующие факторы (причины и условия) совершения компьютерных преступлений:

• компьютерная преступность характеризуется высокой степенью латентности, что обусловлено спецификой данных преступлений, и очень низким количеством сообщений от потерпевших о фактах преступлений;

• малочисленность в правоохранительных органах подготовленных кадров и проблемы квалификации действий преступников;

• высокий материальный ущерб от компьютерных преступлений и преобладание корыстных мотивов их совершения характеризуют компьютерную преступность как корыстную и вредоносную;

• компьютерная преступность зачастую носит транснациональный характер, основанный на стремительном развитии и использовании телекоммуникационных средств и систем получения информации (Internet);

• компьютерная преступность характеризуется высокими темпами развития способов и методов совершения преступлений, которые тесно связаны с резкими темпами роста научно-технического прогресса и компьютерной грамотностью в обществе;

• сокращение высококвалифицированных специалистов, обслуживавших структуры военно-промышленного комплекса (ВПК), различные научно-исследовательские центры, лаборатории и институты; именно за счет такой категории специалистов современная преступность не испытывает недостатка в кадрах, способных эффективно и на высоком уровне использовать новейшие компьютерные системы, электронные средства, свои профессиональные знания и умения в преступных целях;

• стремительный количественный рост преступности и её качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, частой реорганизацией системы правоохранительных органов, несовершенство законодательной базы, серьезные упущения в правоприменительной практике, на наш взгляд, способствуют ускорению процессов развития компьютерной преступности как социального явления [4].

По данным службы безопасности Центробанка (ЦБ) России [5] в период с 2010 по 2019 гг. выявлено и пресечено более 17 000 000 попыток незаконного получения денежных средств с применением компьютеров. Полный ущерб от данного вида преступлений с учетом возможных хищений в коммерческих банках, на рынках ценных бумаг и фондовых биржах оценить практически невозможно. Российское государство терпит колоссальные потери в результате неорганизованности рынка программного обеспечения для электронно-вычислительных машин (ЭВМ). Кража программного обеспечения, разрабатываемого российскими специалистами, по оценкам экспертов, составляет около 90%. Значительные, и вместе с тем никем не определяемые, потери происходят в результате распространения на российском рынке программного обеспечения ЭВМ программных «вирусов». В календарный квартал фиксируется появление от 25 до 35 новых видов компьютерных «вирусов».

Анализ, проведенный Академией Федеральной службы безопасности (ФСБ) России, показал, что в настоящее время наблюдается тенденция образования неформальных групп – так называемых «хакеров» (компьютерных взломщиков), в частности, такие группы могут формироваться и в учебных заведениях. Имеются данные о привлечении «хакеров» к подготовке преступлений, например, в финансовой сфере, на фондовом рынке, с их помощью ведется отслеживание и контроль информации, которая хранится в информационно-справочных и учетных компьютерных системах правоохранительных органов как России, так и зарубежных стран.

На основе анализа специальной литературы по вопросам теории и практики борьбы с компьютерной преступностью выделим три основные группы мер предупреждения компьютерных преступлений, составляющих в своей совокупности целостную систему борьбы с рассматриваемым социально опасным явлением:

а) правовые;

б) организационно-технические;

в) криминологические.

Группу правовых мер предупреждения компьютерных преступлений, в большей степени, составляют нормы законодательства, которые устанавливают уголовную ответственность за противоправные деяния. Первыми нормативными актами, регламентирующими порядок правовой защиты авторских прав на программные средства компьютерной техники и топологии интегральных микросхем в сфере электронно-вычислительной техники, являются Закон РФ от 23.09.1992 г. «О правовой охране программ для электронно-вычислительных машин и баз данных» и «Закон РФ от 23.09.1992 № 3526-I «О правовой охране топологий интегральных микросхем».

Далее принимаются Федеральный закон от 16 февраля 1995 г. № 15-ФЗ «О связи» и Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (на сегодняшний день они утратили силу). Данные нормативные акты позволяли регулировать правовые отношения в сфере информационного обмена и обработки информации, в т.ч. с использованием средств новых информационных технологий.

Самым прогрессивным шагом на пути правового регулирования отношений в сфере высоких технологий, к которым относится и сфера компьютерной информации, по праву считается принятие Уголовного кодекса в 1996 году, устанавливающего уголовную ответственность за компьютерные преступления в России и выделяющего информацию в качестве объекта уголовно-правовой охраны. Данным нормативно-правовым актом отечественное уголовное законодательство приводится в соответствии с общепринятыми международными правовыми нормами.

Следует отметить, что только лишь правовые меры не всегда помогают достичь желаемого результата в предупреждении преступлений, и в этом случае следующим этапом становится применение мер организационно-технического свойства для защиты средств компьютерной техники от противоправных посягательств на них. Эти меры могут играть серьезную общепрофилактическую роль в борьбе с компьютерными преступлениями при их правильном и комплексном использовании.

Отечественные исследователи считают, что «в охране нуждаются не только материальные ценности, но и информационные ресурсы, а контроль за их сохранностью – такая же профилактическая мера в отношении компьютерных преступлений, как и профилактика в любой другой сфере» [6].

На наш взгляд, к организационно-техническим мерам предупреждения компьютерных преступлений является возможным отнесение следующих составляющих:

а) соответствие управленческих процедур требованиям компьютерной безопасности;

б) разработка вопросов технической защиты компьютерных залов и компьютерного оборудования;

в) разработка стандартов обработки данных и стандартов компьютерной безопасности;

г) осуществление кадровой политики с целью обеспечения компьютерной безопасности и ряд других.

С помощью мер технического характера (аппаратные, программные) осуществляется защита компьютерной техники от вредоносных физических воздействий, утечки конфиденциальной информации. Реализуются данные меры при помощи определенных технических устройств, к которым можно отнести источники бесперебойного питания, устройства экранирования аппаратуры, средства охранно-пожарной сигнализации и др. [7]

Существует позиция, что к числу организационно-управленческих мер предупреждения компьютерной преступности относится:

1) предотвращение утечки, хищения, утраты, искажения и подделки информации;

2) предотвращение несанкционированных действий в данной сфере;

3) обеспечение правового режима функционирования документированной информации;

4) сохранение государственной тайны и конфиденциальности документированной информации;

5) обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения и др.

Ряд специалистов выделяют такие меры предупреждения и профилактики компьютерных преступлений, как:

• обеспечение поддержки со стороны руководства конкретной организации, требование защиты средств компьютерной техники;

• разработка комплексного плана защиты информации;

• определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации;

• составление общей сметы расходов финансирования охранных мероприятий в соответствии с разработанным планом и утверждение её в качестве приложения к плану руководством организации;

• определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудником и администрацией предприятия, учреждения, организации и т.п.;

• разработка, внедрение и контроль за исполнением различного рода инструкций, правил и приказов, регламентирующих формы допуска, уровни секретности информации, конкретных лиц, допущенных к работе с секретными данными.

Проанализировав основные меры предупреждения и профилактики борьбы с преступлениями в сфере компьютерной информации, опишем личность преступника, который может совершить противоправные деяния данного вида.

В целом преступник – это человек, совершивший преступление. Данному лицу, как правило, присущи определенные психологические особенности, антиобщественные взгляды, отрицательное отношение к нравственным ценностям и выбор общественно-опасного пути для удовлетворения своих потребностей или непроявления необходимой активности в предотвращении отрицательного результата. Изучение личности преступника осуществляется в основном с целью выявления, анализа и оценки тех её качеств, которые порождают преступное поведение, в целях его профилактики.

Как отмечалось в докладе генерального секретаря Организации Объединенных Наций (ООН), мировой опыт свидетельствует о том, что по мере развития в мире техники и появления специалистов более высокой квалификации «...появляется все больше талантливых людей для изобретения новых уникальных способов совершения преступлений, особенно в области информационно-обрабатывающих технологий» [8].

Проанализировав материал 105 уголовных дел, можем в определенной мере судить о личности преступника, совершившего преступление в сфере компьютерной информации. В данном случае мы обобщаем все преступления, которые подпадают под деяния, обозначенные в главе 28 Уголовного кодекса РФ.

В контрольную группу было включено 50 уголовных дел, по которым проходило 33 преступника. Среди преступников значительно больше мужчин (96%), чем женщин (их доля составляет 4%). Возрастная характеристика преступников позволяет делать выводы о криминогенной активности и особенностях преступного поведения представителей различных возрастных групп, которые разделились следующим образом:

• 14-18 лет – 0%;
• 18-25 лет – 13%;
• 26-30 лет – 21%;
• 31-35 лет –- 29%;
• 36-50 лет – 37%;
• старше 50 лет – 0%.

Значительная часть преступников состояла в официальном (т.е. юридически зарегистрированном) или незарегистрированном браке.

Обратим внимание на уровень образования лиц, совершивших преступления в сфере компьютерной информации. Эти данные распределились следующим образом:

• среднее – 17%;
• незаконченное высшее – 24%;
• высшее – 59%.

По уровню образования лиц, совершивших преступления в сфере компьютерной информации можно с большой долей уверенности сказать, что это одно из самых «интеллектуальных» общественно опасных явлений из всего спектра преступности в России. Практическое большинство преступников занималось трудовой деятельностью, непосредственно связанной с доступом к компьютерному обеспечению.

Их доля составляет около 90%. Из общего числа лиц, привлеченных к уголовной ответственности по изученным делам, около 4% были ранее судимыми. У всех преступников доминировала корыстная цель.

Таким образом, проанализировав особенности уголовно-правовой борьбы с преступлениями в сфере компьютерной информации и IT-технологий, отметим, что профилактика и предупреждение любых, в том числе и компьютерных преступлений, должны носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих структур. С большой долей вероятностью, актуальность и значимость проблем, касающихся научных разработок в области компьютерной безопасности, будет возрастать пропорционально процессу увеличения количества и качества совершаемых компьютерных преступлений.

Следует отметить, что современные уголовно-правовые способы борьбы с компьютерными преступлениями, безусловно, нуждаются в дальнейшем изучении, которое позволит выявить наиболее важные проблемные аспекты и вопросы, что позволит найти наиболее верные пути их решения. Представляется, что значение закрепления в структуре УК РФ преступлений в сфере компьютерной информации обладает повышенной значимостью, так как компьютерные технологии положены в основу работы многих важных систем, которые обеспечивают достойную жизнедеятельность общества и государства.

Библиографический список

1. Ермолаева В.В., Пикина Е.Е. Влияние информационных технологий на жизнь человека // Молодой ученый. 2018. № 22 (208). С. 42-44.

2. Гвоздева В.А. Базовые и прикладные информационные технологии: учебник. М.: ИД «ФОРУМ»; ИНФРА-М, 2019.

3. Карась И.З. Экономический и правовой режим информационных ресурсов. В кн.: Право и информатика. М.: МГУ, 1998. С. 40-59.

4. Методика обучения информационными технологиями: учеб. пособие / А.В. Тараканова, К.В. Садова, Е.А. Крайнова. Самара, 2016.

5. Справочный бюллетень ЦБ России, 2019. С. 13.

6. Черкасов В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 2004. 113 с.

7. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А.В. Аносов и др. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

8. Доклад генерального секретаря ООН «Воздействие организованной преступной деятельности на общество в целом». Материалы Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, 13-23 апреля. E/CN. 15/2016/3.