

*В.А. Мазуров, В.В. Поляков***Криминологическое-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий**

Ключевые слова: криминология, криминалистика, предупреждение, высокие информационные и телекоммуникационные технологии.

Key words: criminology, criminal law, prevention, high information and telecommunication technologies.

Современное информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, экономическими и финансовыми структурами, органами государственной власти [1]. Развитие информационной сферы, обеспечение ее безопасности стало одним из приоритетов национальной политики. Вместе с тем высокие информационные технологии и глобальные компьютерные сети создали условия для преступников, которые изобрели новые способы совершения и сокрытия преступлений не только на национальном, но и международном уровне. Для совершения преступлений в этой области преступниками применяются технические приемы и средства компьютерной техники и используются информационные линии связи, в том числе компьютерные сети. Преступления в информационной сфере сегодня наносят значительный материальный и моральный вред личности, обществу, государству. Анализ состояния, структуры, динамики преступности в сфере высоких технологий позволяет выделить некоторые тенденции и проблемы и сформулировать предложения по ее предупреждению. К таким тенденциям можно отнести:

- качественно-количественные изменения преступности в сфере высоких технологий. Так, с 1997 по 2005 г. включительно отмечается устойчивый рост зарегистрированных преступлений в сфере высоких технологий: 1997 г. – 17; 1998 г. – 67; 1999 г. – 825; 2000 г. – 1375; 2001 г. – 3320; 2002 г. – 6049; 2003 г. – 10920; 2004 г. – 13261; 2005 г. – 14810. С 2006 г. показатель зарегистрированных преступлений в сфере компьютерной информации имеет тенденцию снижения (ст. 272–274 УК РФ): 2006 г. – 14042; 2007 г. – 11622. Вместе с тем с 2002 г. отмечается устойчивая тенденция роста преступлений, совершаемых с использованием ЭВМ, систем и сетей ЭВМ и новейших достижений в сфере высоких технологий, в том числе преступлений, предусмотренных: ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 146 УК РФ «Нарушение

авторских и смежных прав», ст. 159 УК РФ «Мошенничество», ст. 165 УК РФ «Причинение имущественного ущерба путем обмана или злоупотребления доверием», ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 242 УК РФ «Незаконное распространение порнографических материалов или предметов», ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма» и ряд других преступлений. Известен случай доведения до самоубийства (ст. 110 УК РФ), когда группа молодых людей, хорошо владеющих компьютерными технологиями, в течение пяти лет размещала в Интернете компрометирующую информацию на своего сверстника, устроила тотализатор, где ставили на его жизнь, в результате он покончил жизнь самоубийством [2].

Учитывая указанную тенденцию, а также стремительное развитие научно-технического прогресса, можно спрогнозировать на ближайшую перспективу увеличение и качественное изменение преступлений, совершаемых с использованием ЭВМ, системы, сети ЭВМ и новейших высоких технологий, а именно:

- активизацию противоправной деятельности организованных преступных групп и сообществ с использованием достижений научно-технического прогресса и, прежде всего, в финансово-банковской, информационной, экономической сферах, совершении преступлений террористической, экстремистской направленности, против собственности, в том числе интеллектуальной;

- высокий уровень латентности;
- транснациональный характер преступлений;
- поведение определенной категории организаций-потерпевших, скрывающих факт совершения преступления и противодействующих его расследованию в целях сохранения деловой репутации.

Указанные тенденции предопределили проблемы, связанные с предупреждением преступности в сфере высоких информационных и телекоммуникационных технологий, к которым можно отнести следующее.

1. Несовершенство правовой базы, отставание законодательного обеспечения борьбы с преступностью в сфере высоких технологий. Так, до настоящего времени не приняты законы, определяющие правовой статус охраняемой законом информации, в том числе предусмотренные в качестве первоочередных мер совершенствования правовой базы в

Основных направлениях нормативного правового обеспечения информационной безопасности Российской Федерации (2001 г.) – ФЗ «О праве на информацию», ФЗ «О неприкосновенности частной жизни, личной и семейной тайны», ФЗ «О служебной тайне», ФЗ «О защите нравственности» и ряд других законов. Принятые нормативные правовые акты, такие как ФЗ «О коммерческой тайне» от 29 июля 2004 г., ФЗ «О персональных данных» от 27 июля 2006 г., на наш взгляд, имеют некоторые недостатки, в частности, относительно законодательного определения «коммерческой тайны», «персональных данных». Имеются замечания и по структуре данных законов. Аналогичные проблемы имеют место и в проекте ФЗ «О служебной тайне».

2. Проблема реализации принятых законов на практике, которая заключается в неразработанности механизма применения положений этих нормативных актов, в том числе несвоевременное внесение дополнений и изменений в действующее административное, гражданское, уголовное законодательство, принятие различного рода подзаконных актов, обеспечивающих реализацию принятых законов, распоряжений, инструкций и других документов министерств, ведомств, иных федеральных и региональных органов государственной власти. Подтверждение этому получено в результате проведенного опроса государственных служащих, сотрудников правоохранительных органов, предпринимателей Барнаула, слушателей курсов повышения квалификации Центра повышения квалификации и переподготовки в области международной и национальной безопасности Алтайского госуниверситета.

3. Недостаточный уровень системы образования, воспитания, правовой и профессиональной подготовки кадров в сфере высоких технологий, способных компетентно противодействовать преступлениям и правонарушениям.

4. Недостаточный уровень научно-исследовательской работы по изучению проблем противодействия преступности в сфере высоких информационных и телекоммуникационных технологий на национальном и международном уровнях.

С учетом указанных проблем можно выделить следующие приоритетные направления по предупреждению правонарушений и преступлений в сфере высоких технологий:

- совершенствование нормативной правовой базы и механизма реализации действующих законов, регулирующих отношения в информационной сфере и защиту информации путем оценки эффективности применения действующих нормативных правовых актов, разработки и принятия указанных выше федеральных законов;

- разработка федеральной целевой программы по противодействию преступности в сфере высоких

технологий, на ее основе разработка и реализация региональных программ;

- повышение уровня научно-исследовательской работы на национальном и международном уровнях; совершенствование работы по подготовке научных кадров и специалистов по обеспечению информационной безопасности для органов государственной власти, правоохранительных органов, в сфере предпринимательской деятельности.

Учитывая транснациональный характер преступности в сфере высоких технологий, устойчивую тенденцию качественно-количественных изменений данной преступности, а также рекомендации, предложения, задачи и направления их реализации, изложенные в Стратегии, других официальных документах, представляется целесообразным создание организации по исследованию международной преступности в целом и в сфере высоких технологий, в частности, объединяющей ученых юридических и технических специальностей. В Алтайском государственном университете в целях совершенствования научной и учебно-методической деятельности, повышения качества подготовки студентов юридического и физико-технического факультетов, подготовки, переподготовки и повышения квалификации практических сотрудников органов государственной власти в 2006 г. был создан Региональный научно-методический центр правовой и технической защиты информации (РНМЦ). На физико-техническом факультете открыта новая специальность «Комплексное обеспечение информационной безопасности автоматизированных систем». На юридическом факультете введены спецкурсы «Криминология-криминалистические основы информационной безопасности», «Уголовно-правовая защита тайны», «Организационно-правовые основы информационной безопасности». Членами РНМЦ опубликовано 25 научных трудов, статей в научных журналах, тезисов выступлений на международных и всероссийских конференциях, в которых сформулированы конкретные предложения по совершенствованию действующего законодательства и правоприменительной практики. На кафедре уголовного процесса и криминалистики проведено научное исследование особенностей расследования неправомерного удаленного доступа к компьютерной информации. В 2008 г. в соответствии с планами работы Алтайского отделения «Ассоциация юристов России» и РНМЦ в АлтГУ проведен научно-практический семинар «Проблемы правовой и технической защиты информации», в работе которого приняли участие преподаватели юридических и технических факультетов вузов России, Республики Казахстан, ответственные сотрудники органов государственной власти, правоохранительных органов, представители общественных организаций. По результатам работы семинара был опубликован сборник научных статей преподавателей вузов России и практических работников. Участниками семинара высказаны конкретные предложения по совершенствованию работы

по предупреждению правонарушений и преступлений в сфере высоких технологий. Отмечена необходимость комплексного подхода к решению проблем правовой и технической защиты информации, подготовке научных кадров, специалистов по обеспечению информационной безопасности путем консолидации ученых и преподавателей юридических и технических факультетов, ответственных сотрудников органов государственной власти, правоохранительных органов [3].

Предупреждение преступлений является одним из наиболее эффективных путей борьбы с преступностью и представляет собой весьма сложный и многоплановый комплекс мер различного характера. Одной из основных частей этого комплекса является криминалистическое предупреждение преступлений. Криминалистическое предупреждение – это система «научных положений и практических рекомендаций о закономерностях разработки и использования в уголовном судопроизводстве технических средств, тактических и методических приемов для предотвращения подготавливаемых преступлений», а также «своевременного обнаружения, полного раскрытия и качественного расследования совершенных преступлений, выявления и устранения в процессе расследования обстоятельств, способствующих совершению и раскрытию преступлений» [4].

Отметим, что в последнее время большинство ученых сошлись во мнении, что понятия «предупреждение преступлений» и «профилактика преступлений» имеют очень близкое содержание, поэтому используют данные понятия как синонимы. В другом важном вопросе, касающемся соотношения криминалистического и криминологического предупреждения в науке нет единства точек зрения. По мнению М.Ш. Махтаева, не существует четкой границы между криминологическим и криминалистическим предупреждением преступлений, подобно тому, как не существует жесткого разграничения между криминалистикой и уголовным процессом [5]. Об отсутствии такого разграничения «в силу взаимного влияния и проникновения» писал также Р.С. Белкин [6]. Ранее аналогичную позицию отстаивал В.Ф. Зудин, писавший, что «четкой границы в сфере криминологической и криминалистической профилактики нет» [7]. В то же время И.И. Иванов выступает против подобного расширения рамок криминалистической профилактики, позицию которого мы поддерживаем. По сути, это отражает различные взгляды на предмет криминалистического предупреждения преступлений. На наш взгляд, можно выделить положения, объединяющие различные точки зрения и заключающиеся в том, что теоретической и прикладной проблематикой криминалистического предупреждения преступлений является разработка средств, методов и приемов, использование которых способно обеспечить эффективное осуществление комплекса предупредительных мероприятий. Проблематика криминалистического предупреждения преступлений

имеет пограничный характер, получаемые результаты представляют ценность как непосредственно для криминалистики, так и для уголовного процесса и теории оперативно-разыскной¹ деятельности. Как следствие, разрабатываемые приемы и методы применяются, во-первых, следователями и органами дознания; во-вторых, оперативными работниками; в-третьих, специалистами и экспертами; в-четвертых, сотрудниками прокуратуры; в-пятых, сотрудниками суда.

Исследователи, занимающиеся проблемами криминалистического предупреждения преступлений, справедливо указывают на то, что лишь в небольшом числе научных публикаций, диссертаций, учебно-методических работ по криминалистике уделяется внимание вопросам предотвращения преступлений [4]. Другими словами, внимание специалистов к профилактической деятельности, осуществляемой средствами криминалистики, явно ослаблено. Неработанность теории наиболее заметна для «молодых» видов преступности, связанных с привлечением высоких технологий, прежде всего с преступлениями в сфере высоких информационных и телекоммуникационных технологий. Так, отсутствуют даже в постановке исследования, посвященные криминалистическому предупреждению преступлений, осуществляемых с помощью неправомерного удаленного доступа к компьютерной информации.

Особую значимость для развития теории и для нужд практики имеет построение системы классификации мер по обеспечению криминалистического предупреждения преступлений. Предупреждение преступлений, совершенных с использованием компьютерной техники и технологий, может быть подразделено на группы мер правового, технического, организационного и методического характера [8]. Данные меры имеют комплексный характер и должны быть реализованы при их сочетании.

К правовым мерам относятся разработка и принятие новых, изменение и совершенствование существующих норм законодательства.

В последнее время сотрудниками правоохранительных органов, непосредственно занимающихся расследованием неправомерного доступа к компьютерной информации, высказывается мнение о необходимости ужесточить наказания за данные преступления из-за их повышенной общественной опасности.

Положительную роль сыграли бы различные мероприятия в средствах массовой информации, освещающие вопросы ответственности за преступления в сфере компьютерной информации. Это связано с тем, что большой группой преступников является талантливая молодежь, которая не в полной мере осознает,

¹ Написание слова *оперативно-разыскной* дано в соответствии с современными правилами русского языка. См.: Правила русской орфографии и пунктуации. Полный академический справочник (под ред. В.В. Лопатина. М., 2006. С. 53 (§ 40). – *Прим. ред.*

что их действия влекут уголовную ответственность.

При анализе группы мер, связанных с организационной деятельностью, представляется полезным выделить два основных направления: меры, направленные на совершенствование работы правоохранительных органов, и меры, относящиеся к организации деятельности конкретных организаций и физических лиц.

Отдельной, причем не терпящей отлагательства задачей является организация действенной системы подготовки кадров для соответствующих подразделений правоохранительных органов (прежде всего в системе МВД).

Организационные меры профилактики и предупреждения преступлений в сфере компьютерной информации и неправомерного доступа к компьютерной информации, в частности, совершаемые в организациях, можно подразделить на внутренние и внешние. Внутренние меры направлены на предотвращение преступлений со стороны персонала. Внешние – на профилактику проникновения к компьютерной технике и информации со стороны посторонних лиц, например, использующих возможности удаленного сетевого соединения.

Для реализации мер, отнесенных нами к внутренней группе, необходимо следовать правилам комплексного обеспечения информационной безопасности автоматизированных систем. Необходим тщательный подбор персонала, проведение регулярных проверок и инструктажей, возложение ответственности за информационную безопасность на специально обученных лиц. Требуется также обеспечение режима секретности, продуманная организация охраны рабочих мест и помещений. Исследование уголовных дел показывает, что к наиболее распространенным причинам, приводящим к совершению преступлений, часто относится именно пренебрежение мерами внутренней безопасности (свободный доступ персонала к компьютер-

ной технике, низкий уровень корпоративной этики, отсутствие специальной службы, обеспечивающей информационную безопасность).

Предотвращению преступлений способствует применение одноразовых или хорошо зашифрованных паролей.

Технические меры включают в себя разработку и использование программно-аппаратных методов и средств защиты информации. Аппаратные средства включают в себя технические устройства для защиты средств компьютерной техники и сетевых средств связи от нежелательных воздействий, а также для перекрытия физических каналов утечки информации. К ним относятся электронные ключи, электронные замки, средства для предотвращения незаконного подключения к линиям проводной связи, устройства экранирования и т.д. Программные меры включают в себя соответствующее программное обеспечение, в частности, экраны (брандмауэры) по защите компьютеров и локальных сетей, программы для криптографической защиты и т.д.

Разработка научно обоснованной политики в области борьбы с преступлениями в сфере компьютерной информации является методической основой предотвращения их распространения. Для этого требуется как создание общей методологии, так и разработка конкретных методик такой деятельности. Сюда же относится разрешение проблемы отсутствия надежных и эффективных методик расследования преступлений в сфере компьютерной безопасности, методик проведения компьютерно-технических экспертиз и т.д.

Предупреждение преступлений в сфере высоких технологий является сложной комплексной задачей. Решение ее начинается с выявления имеющихся проблем в этой области и заканчивается выработкой и применением конкретных мер по устранению причин и условий совершения данных преступлений.

Библиографический список

1. Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 // Российская газета. – 2008. – 16 февр.
2. Новоселова, Е. Унизить до смерти. В Интернете устроили тотализатор, где ставили на жизнь подростка / Е. Новоселова // Российская газета. – 2008. – 17 сент.
3. Проблемы правовой и технической защиты информации : сб. науч. ст. – Барнаул, 2008.
4. Иванов, И.И. Криминалистическая превенция (генезис, теоретические и методологические основы, перспективы развития в сфере нового уголовно-процессуального законодательства) / И.И. Иванов. – СПб., 2003.
5. Махтаев, М.Ш. Основы теории криминалистического предупреждения преступлений / М.Ш. Махтаев. – М., 2001.
6. Белкин, Р.С. Курс криминалистики : в 3 т. Т. 3: Криминалистические средства, приемы и рекомендации / Р.С. Белкин. – М., 1997.
7. Зудин, В.Ф. Социальная профилактика преступлений: Криминологические и криминалистические проблемы / В.Ф. Зудин ; под ред. В.И. Федулова. – Саратов, 1983.
8. Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации : сб. науч. ст. – Барнаул, 2008.