УДК 343.98
ББК 67.404.9

А.А. Протасевич,
доктор юридических наук, профессор,
Байкальский государственный университет экономики и права
Л.П. Зверянская,
Байкальский государственный университет экономики и права

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ КАК АКТУАЛЬНАЯ ЗАДАЧА СОВРЕМЕННОЙ НАУКИ

В статье авторы делают акцент на глобальности проблемы киберпреступлений, указывая масштабность деятельности киберпреступников.

Анализируя российское законодательство, регламентирующее ответственность за преступления в сфере компьютерной информации, авторы обращают внимание на пробелы уголовного законодательства. Как один из вариантов решения этой проблемы предлагается принятие Конвенции о киберпреступности, обосновывается это тем, что нормы, содержащиеся в Конвенции, способны дополнить и улучшить законодательную базу нашего государства в этой сфере.

Официальная статистика состояния киберпреступности в России за 2000–2010 годы демонстрирует противоречивую динамику, что связано с различными методиками подсчета количества преступлений правоохранительными органами, а также с высокой латентностью данного вида преступлений.

В итоге авторы приходят к нескольким выводам: недостаток комплексных исследований и высокая латентность привели к неэффективности существующих мер предупреждения данного вида преступлений; для решения проблемы киберпреступности требуется международное сотрудничество, так как данный вид преступлений не признает никаких границ; существует необходимость создания новых органов и организаций, осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, которые можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью.

Ключевые слова: киберпреступность; компьютерные преступления; преступления в сфере информационных технологий; борьба с киберпреступностью.

A.A. Protasyevich,
Doctor of Law, Professor,
Baikal National University of Economics and Law
L.P. Zveryanskaya,
Baikal National University of Economics and Law

FIGHTING CYBERCRIMES AS AN URGENT TASK FOR CONTEMPORARY RESEARCH

The authors of the paper stress the global character of cybercrimes issue and point out the large scale of cybercriminals' activities.

Having analyzed Russian legislation that regulates liability for crimes in the sphere of computer information the authors draw attention to the gaps in criminal legislation. They suggest adopting the Cybercrime Convention as one of the ways to bridge these gaps because the norms of the Convention could supplement and improve the legislative base in this sphere.

The official statistics of cybercrimes in Russia in 2000–2010 show contradictory dynamics, which is connected with different methodologies used by law enforcement bodies to calculate the number of such crimes as well as with their high latency.

At the end the authors draw several conclusions: lack of comprehensive research and high latency render the existing prevention measures for these crimes ineffective; international cooperation is necessary to resolved the problem of cybercrimes because this type of crimes knows no borders; it is necessary to form new bodies and agencies that would fight cybercrimes which, in its turn, requires a national training program to prepare specialists for transnational bodies and organizations fighting cybercrimes.

Key words: cybercrimes; computer crimes; crimes in the sphere of information technologies; fighting cybercrimes.

В настоящее время борьба с киберпреступностью является одной из наиболее актуальных проблем во всем мире. Растущее количество киберпреступников, постоянное совершенствование информационных технологий и, как следствие, новые возможности «совершенствования» этих преступлений создают очередные угрозы для глобальных информационных сетей и общества в целом.

Уже никого не удивляют ежедневные публикации СМИ о новых фактах судебных разбирательств по делам о киберпреступлениях, в частности, по делам о кибермошенничествах. Но мало кто обращает внимание на то, что преступники не останавливаются только на разработке мошеннических схем. По данным компании-разработчика антивирусного программного обеспечения McAfee, системы газового, электрического и водяного снабжения уже давно подвергаются подобным нападениям. McAfee провела исследование 200 IT-отделов* 14 стран, отвечающих за снабжение жизненно важными ресурсами, согласно которому был сделан вывод о том, что 80 % IT-отделов были подвергнуты посягательствам в прошлом году. Если только представить, что хакеры могут завладеть информационными технологиями в области энергетики, химической промышленности, нефтегазовых объектов, нарушить системы водоснабжения, то последствия и ущерб будет оценить уже достаточно трудно. Радует только то, что по прогнозам специалистов такое критическое положение может возникнуть еще не скоро, хотя именно сейчас хакеры пробуют себя в этих отраслях, нарабатывая опыт и методики такого вида посягательств.

Ни для кого уже не секрет, что наша страна является одним из лидеров по числу кибер-атак во всем мире, два других «почетных» места занимают США и Китай. Это происходит потому, что российские законы, регулирующие вопросы киберпространства и преступных посягательств, недостаточно разработаны.

В этой связи хотелось бы отметить следующее.

В Российской Федерации ответственность за преступления в сфере компьютерной информации регламентируется главой 28 УК РФ. Компьютерные преступления охватываются тремя составами, а именно, неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием и распространением вредоносных программ для ЭВМ (ст. 273 УК РФ) и нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). С момента принятия Уголовного кодекса Российской Федерации прошло 15 лет, и за это время не было внесено ни одного дополнения или изменения в главу 28 УК РФ. Развитие компьютерных технологий предоставило возможность совершения киберпреступлений практически безнаказанно, поскольку в настоящее время уголовное законодательство не адаптировано к новым видам преступлений в сфере информационных технологий.

Для сравнения можно привести уголовное законодательство, регламентирующее ответственность в сфере киберпреступности Германии, которое постоянно совершенствуется и модифицируется, так, например, неоднократно менялась дефинитивная часть уголовно-правовых норм, регулирующих киберпреступления, последние изменения имели место в 2007 году [7, с. 10].

Между тем за последние 15 лет уже не раз вставал вопрос об усовершенствовании законодательства, регулирующего сферу компьютерных технологий. Многие ученые, занимающиеся данной проблематикой, периодически предлагали различные поправки и дополнения к существующим нормам, но в основном законодатель не прислушивался к их мнению.

В настоящее время активно обсуждаются внесенные в Госдуму поправки к закону о «спаме» (массовая электронная рассылка). Законопроект был подготовлен думским Комитетом по информационной политике, информационным технологиям и связи совместно с Комиссией по информационной безопасности и киберпреступности Российской Ассоциации Электронных Коммуникаций (РАЭК).

Проект предполагает внесение изменений в федеральные законы «Об информации, информационных технологиях и о защите информации», «О связи», в Кодекс об административных правонарушениях и Уголовный кодекс РФ.

---

* IT (Information Technology) – информационные технологии.

Поправки, в частности, предлагают введение уголовной ответственности за массовую (1 тыс. писем в течение дня или 10 тыс. за неделю) рассылку спама. Нарушителю грозит либо штраф до 1 млн руб., либо обязательные работы сроком от 120 до 180 часов, либо исправительные работы на срок от шести месяцев до года. Если же нарушение совершено группой лиц по предварительному сговору или с извлечением дохода в особо крупном размере (более 100 тыс. руб.), им будет грозить штраф до 2 млн руб. либо обязательные или исправительные работы от 180 до 240 часов и от года до двух соответственно.

Аналогичные штрафы предусмотрены за производство, распространение и использование компьютерных программ, которые автоматически собирают, обрабатывают и распространяют адреса электронной почты. Соответствующие статьи предлагается добавить в Кодекс РФ об административных правонарушениях.

Данные поправки к законам должны облегчить жизнь всем пользователям электронной почты, но и у них уже сейчас выявлены недочеты: некоторые эксперты полагают, что предложенные поправки чрезмерно ограничивают свободу информации, а для введения уголовной ответственности за рассылку спама придется серьезно проработать вопрос о том, как доказывать совершение этого преступления, – для этого придется как минимум обязать операторов связи и интернет-ресурсов хранить историю о рассылках в течение определенного времени [4].

В 2008 году Российская Федерация отказалась от подписания европейской Конвенции о Киберпреступности. Соответствующее распоряжение поступило от Президента РФ, так как нашей стране не удалось договориться о приемлемых условиях трансграничного доступа к компьютерным системам (хотя на данный период Конвенцию уже подписали 46 стран и ратифицировали в 24 странах).

Сегодня можно утверждать, что необходимость подписания и ратификации Конвенции осталась, так как российское уголовное законодательство нуждается в кардинальных изменениях, а Конвенция содержит в себе нормы, способные дополнить и улучшить законодательную базу нашего государства в этой сфере.

Конвенция о киберпреступности направлена на регулирование трех основных вопросов:

– уголовно-правовой характеристики преступлений в сфере компьютерной информации;

– уголовно-процессуальных аспектов борьбы с преступностью, направленных на обеспечение собирания доказательств при расследовании компьютерных преступлений;

– международного сотрудничества в уголовно-процессуальной деятельности, направленной на собирание доказательств совершения таких преступлений за рубежом [1, с. 18].

Также Конвенция о Киберпреступности называет 5 видов компьютерных преступлений:

– незаконный доступ (противоправный умышленный доступ к компьютерной системе либо ее части);

– незаконный перехват (противоправный умышленный перехват непредназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные);

– вмешательство в данные (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

– вмешательство в систему (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных);

– незаконное использование устройств (производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование: устройств, включая компьютерные программы, разработанных или адаптированных для совершения преступлений; компьютерных паролей, кодов доступа или иных подобных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой её части, с целью использовать их для совершения преступлений. А также владение одним из предметов, упоминаемых выше, с намерением использовать его с целью совершения преступлений).

Возникновение данного вида преступ-

лений требует введения специальной терминологии, которая будет единой как для правоохранительных органов, так и для IT-специалистов. Многие понятия, входящие в IT-лексикон, давно используются в современном мире, например, такие как *киберпространство, кибертерроризм*, но подходы представителей технических и юридических отраслей науки к каждому термину различны.

На данный момент, на пике роста киберпреступлений, не выведено единого общепризнанного понятия киберпреступности. Согласно рекомендациям экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети. Иначе говоря, к киберпреступлениям относятся такие общественно опасные деяния, которые совершаются в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных.

Для решения данной проблемы необходимо на законодательном уровне дать разъяснения по каждому из приведенных терминов, как это сделано в США. Верховный Суд США дал разъяснения понятия «киберпространства» – «уникальной среды, не расположенной в географическом пространстве, но доступной каждому в любой точке мира посредством доступа в Интернет» [2, с. 20], а также был принят закон «PATRIOT ACT 2001», содержащий в себе трактовку кибертерроризма.

Официальная статистика недостаточно точно отражает характеристику структуры, состояния и динамики современной российской киберпреступности (табл.)

Анализ приведенных данных показывает, что наибольший рост преступлений был в 2005 и 2009 годах. Достаточно трудно объяснить рост числа зарегистрированных преступлений в 2005 году и последовавший за этим спад в регистрации на 13 %, а в дальнейшем еще на 18,6 %. Также непонятно снижение этих показателей в 2010-м на 36,4 %. Такое изменение регистрации компьютерных преступлений за указанный период демонстрирует противоречивую динамику, несмотря на то, что законодательство в этой сфере не менялось, а информационные технологии развивались достаточно быстрыми темпами. Можно предположить, что причины резких перепадов уровня киберпреступности вызваны не фактическим состоянием преступности, так как общая тенденция – это рост числа

Таблица

Количество зарегистрированных преступлений в сфере компьютерной информации в России за 2000–2010 гг.

Показатель	Год										
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Количество зарегистрированных преступлений в сфере компьютерной информации	852	2133	4050	7540	8739	10214	8889	7236	9010	11636	7398
Темпы прироста (базисный способ), %	–	+150	+375,3	+784,9	+925,7	+1098,8	+943,3	+749,2	+957,5	+1265,7	+768,3
Темпы прироста (цепной способ), %	–	+150	+89,8	+86,1	+15,9	+16,9	–13	–18,6	+24,5	+29,1	–36,4

киберпреступлений, а изменениями в правовой политике государства, ведомств, органов, занимающихся выявлением, учетом, расследованием и раскрытием данной категории преступлений. Полагаем также, что это связано с различными методиками подсчета количества указанных преступлений правоохранительными органами [6, с. 126].

Структурный анализ преступности в сфере компьютерной информации показывает, что наиболее распространенными деяниями являются: неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ и нелицензионного программного обеспечения, посягательства на электронно-платежные системы, а также распространение порнографических материалов с участием несовершеннолетних в сети Интернет.

Тем не менее специалисты утверждают, что латентность данного вида преступлений составляет примерно 80–90 % и выше. Так, например, М.В. Старичков называет уровни латентности: 99,7 % по ст. 272 УК РФ и 99,8 % по ст. 273 УК РФ [5, с. 109–112].

Из-за высокой латентности киберпреступности для установления истинных масштабов ее распространения требуется использование новых методов и источников получения информации (по последним оценкам, потери от компьютерных преступлений в глобальном масштабе составляют 750 млрд евро в год) [3].

Получение и анализ доказательств по делам о преступлениях в сфере компьютерной информации – одна из самых основных и трудно решаемых на практике задач для всех государств. Ее решение требует не только разработки тактики производства следственных и организационных мероприятий, но и наличия специальных знаний в области компьютерной техники и программного обеспечения, а также внесения поправок в действующее уголовно-процессуальное законодательство. По этой причине следует обратить внимание на ст. 102 Основ законодательства Российской Федерации о нотариате «Обеспечение доказательств, необходимых в случае возникновения дела в судах или административных органах», которая гласит: «По просьбе заинтересованных лиц нотариус обеспечивает доказательства, необходимые в случае возникновения дела в суде или административном органе, если имеются основания полагать, что представление доказательств впоследствии станет невозможным или затруднительным». Данная норма позволяет нотариусам обеспечивать доказательства в сети Интернет, но, к сожалению, эта услуга не является востребованной, хотя уже сейчас имеется несколько прецедентов.

Лица, занимающиеся расследованием данного рода преступлений, и работники судебной системы в большинстве своем не обладают специальными познаниями в области новых компьютерных технологий, что влечет ошибки в квалификации и расследовании преступлений. Также причинами ошибок является отсутствие достаточного количества рекомендаций и разъяснений по расследованию преступлений в сфере информационных технологий, отсутствие обобщенной судебной практики по киберпреступности и отсутствие в правоохранительных органах необходимого числа специалистов, разбирающихся в современной технике и способных оперативно выявлять и расследовать компьютерные преступления. В этой связи возникает задача введения новых специализаций и внесения изменений в учебный план подготовки студентов юридических вузов, курсантов и слушателей специальных учебных заведений.

Недостаток комплексных исследований и высокая латентность приводят к неэффективности существующих мер предупреждения данного вида преступлений.

В отличие от всемирной паутины, которая не признает национальных границ и является по своей природе трансграничной, национальные законодательства и правоохранительные органы различных стран в своей деятельности вынуждены принимать во внимание особенности границ, языковые, политические, религиозные особенности, влияющие на эффективность борьбы с преступностью данного вида. Специфичность характеристик требует межгосударственного подхода к противодействию киберпреступлениям, эффективность которого недостижима без международного сотрудничества.

Необходимо также обратить внимание на то, что зарубежные страны с каждым годом увеличивают число служб и ведомств для противодействия киберпреступности, поэтому стоит изучить и перенять их опыт.

Например, в США созданы такие ведомства, как US Cyber Command (военное подразделение, которое осуществляет свою деятельность в киберпространстве), United States Computer Emergency Readiness Team (Национальный отдел киберзащиты Департамента внутренней безопасности США), Computer Crime and Intellectual Property Section (Отдел компьютерной преступности и интеллектуальной собственности), Internet police (Интернет-полиция, сетевая полиция); в Эстонии в 2006 году создана компьютерная группа реагирования на чрезвычайные ситуации (CERT-EE).

Сегодня в России на повестке дня стоит вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей, которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Волеводз А.Г.* Конвенция о Киберпреступности: Новации Правового Регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17–25.

2. *Дашян М.* Обзор Конвенции Совета Европы о киберпреступности // Современное право. – 2002. – №11. – С. 20–24.

3. *Левашова Ю.* Европол оценивает ущерб от хакеров в 750 миллиардов евро в год. – URL : http: // www. crime-research.ru /news/ 05.01.2011 /7060. htm

4. РАЭК отправил в Госдуму новый бессмысленный закон о спаме. – URL : http: // webplanet.ru/ news/ law/ 2011/ 05/ 16/ antispam_law . html

5. *Старичков М.В.* Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. ... канд. юрид. наук. – Иркутск, 2006. – С. 109–112.

6. *Суслопаров А.В.* Компьютерные преступления как разновидность преступлений информационного характера : дис. ... канд. юрид. наук. –Красноярск, 2010. – 210 с.

7. *Тропина Т.Л.* Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : монография. – Владивосток, 2009. – 237 с.

REFERENCES

1. Volevodz A.G. *Pravovye voprosy svyazi* [Legal Issues of Communications]. 2007, no. 2, pp. 17–25.

2. Dashyan M. *Sovremennoe pravo* [Contemporary Law]. 2002, no. 11, pp. 20–24.

3. Levashova Yu. *Evropol otsenivaet ushsherb ot khakerov v 750 milliardov evro v god* [Europol Estimates Damage from Hacking at EUR 750 bln. a Year]. Available at: http: // www. crime-research.ru /news/ 05.01.2011 /7060. htm

4. *RAEK otpravil v Gosdumu novyy bessmyslennyy zakon o spame* [RAEC Sends a New Pointless Antispam Law to the State Duma]. Available at: http: // webplanet.ru/ news/ law/ 2011/ 05/ 16/ antispam_law. html

5. Starichkov M.V. *Umyshlennye prestupleniya v sfere komp'yuternoy informatsii: ugolovno-pravovaya i kriminologicheskaya kharakteristiki (dis. kand. nauk.)* [Deliberate Crimes in the Sphere of Computer Information: Criminal Law and Criminological Characteristics (Cand. Dis. Thesis)]. Irkutsk, 2006, pp. 109–112.

6. Susloparov A.V. *Komp'yuternye prestupleniya kak raznovidnost' prestupleniy informatsionnogo kharaktera (dis. kand. nauk.)*[Computer Crimes as a Type of Information Crimes (Cand. Dis. Thesis)]. Krasnoyarsk, 2010, 210 p.

7. Tropina T.L. *Kiberprestupnost'. Ponyatie, sostoyanie, ugolovno-pravovye mery bor'by* [Cybercrimes. Concept, Condition, Criminal Law Measures for Fighting it]. Vladivostok, 2009, 237 p.

Информация об авторах

Протасевич Александр Алексеевич (Иркутск) – доктор юридических наук, профессор, заслуженный юрист Российской Федерации, декан судебно-следственного факультета. ФГБОУ ВПО «Байкальский государственный университет экономики и права» (664003, г. Иркутск, ул. Ленина, 11, e-mail: irkcenter@isea.ru)

Зверянская Лариса Павловна (Иркутск) – аспирант кафедры уголовного процесса и криминалистики. ФГБОУ ВПО «Байкальский государственный университет экономики и права» (664003, г. Иркутск, ул. Ленина, 11, e-mail: zveryanskayal@mail.ru)

Information about the authors

Protasyevich, Alexander Alekseyevich (Irkutsk) – Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Dean, Department of Judicial Inquiry. Baikal National University of Economics and Law (Lenin st., 11, Irkutsk, 664003, e-mail: irkcenter@isea.ru)

Zveryanskaya, Larisa Pavlovna (Irkutsk) – Ph.D. student, Chair of Criminal Process and Criminalistics. Baikal National University of Economics and Law (Lenin st., 11, Irkutsk, 664003, e-mail: zveryanskayal@mail.ru)