КИБЕРПРЕСТУПНОСТЬ: ОСНОВНЫЕ ПРОЯВЛЕНИЯ И ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ

© 2014 Глотина Ирина Михайловна
Пермская государственная сельскохозяйственная академия
614990, г. Пермь, ул. Петропавловская, д. 23
E-mail: glotina-i@yandex.ru

Определены основные факторы, влияющие на рост числа киберпреступлений, выделены субъекты киберпреступлений, их мотивы, используемое информационное оружие. Выявлены особенности киберпреступности и ее влияние на экономику государств. Показан объем различных сегментов рынка киберпреступности.

Ключевые слова: информационные технологии, киберпреступления, виды киберугроз, анализ рынка киберпреступлений.

Стремительное развитие компьютерных, в том числе интернет-технологий, их активное использование во всех сферах экономической деятельности стали важнейшей тенденцией развития современного общества. Растущее применение интернет-технологий для организации торговли ценными бумагами, расширение сферы электронных расчетов, интернет-коммерции, автоматизации многих функций в сфере бизнеса порождают и новую специфическую область криминальной активности. В условиях наращивания в мире процессов глобализации и формирования "информационного общества" в качестве самостоятельного фактора, способного угрожать экономической безопасности, стала выступать компьютерная преступность.

Активное внедрение информационных технологий во все сферы деятельности привели к изменению и перечня преступлений, относимых к экономическим. К этим преступлениям стали относить компьютерные преступления, причиняющие вред экономике государства, ее отдельным секторам, предпринимательской деятельности, а также экономическим интересам отдельных групп граждан.

По оценкам специалистов, в США ежегодно потери корпораций от преступности превышают 200 млрд, а от компьютерных преступлений - 6 млрд долл. В Великобритании компьютерные преступления обходятся в 2 млн ф. ст. в день. По словам главы Бюро специальных технических мероприятий (БСТМ) МВД России А. Мошкова, компьютерные преступления в России с каждым годом совершаются все чаще, по данным за 2013 г., их число увеличилось на 8,6 %. Общий ущерб от выявленных в России киберпреступлений в 2012 г. составил более 70 млн руб. По оценкам ряда исследований, каждую секунду в мире жертвами киберпреступников становятся 12 чел., и эта цифра с каждым годом растет[1].

Можно выделить следующие факторы, влияющие на рост числа киберпреступлений:

- глобальная информатизация всех сфер жизни общества не повышает, а понижает степень его безопасности;

- ускорение научно-технического прогресса увеличивает вероятность применения преступниками в качестве средств поражения сугубо мирных технологий, причем возможность "двойного" их использования часто не только не предусматривается, но и не осознается создателями технологии;

- терроризм все более становится информационной технологией особого типа, поскольку: во-первых, террористы все шире используют возможности современных информационно-телекоммуникационных систем для связи и сбора информации; во-вторых, реалией наших дней становится так называемый "кибертерроризм"; в-третьих, большинство террористических актов сейчас рассчитаны не только на нанесение материального ущерба и угрозу жизни и здоровью людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей;

- "цифровое неравенство" и появление "проигравших" информационную гонку стран могут послужить причиной террористической активности против отдельных государств как средство асимметричного ответа.

Субъектами преступлений, активно использующими высокие технологии, наряду с лицами, выполняющими профессиональные функции в организациях и на предприятиях, становятся практически любые лица. При этом преследуемые ими цели, используемые методы и располагаемые ими возможности практически не отличаются от тех, которые присущи преступникам по роду занятости.

Основным мотивом киберпреступников выступает извлечение материальной выгоды. По результатам ежегодного исследования компании Symantec ущерб от киберпреступности, нанесенный мировой экономике за 2013 г., оценивается в 113 млрд долл. в год во всем мире и в 2 млрд долл. в год в России[2].

Основными объектами киберугроз являются граждане, бизнес-структуры и государство (см. таблицу).

Объекты и виды киберугроз

Объект угроз	Виды угроз
Граждане	Воздействие на личность путем сбора персональных данных и атак на персональные компьютеры и мобильные устройства граждан, утечка и обнародование частной информации, мошенничество, распространение опасного контента
Бизнес	Воздействие на системы интернет-банкинга, воздействие на информационную инфраструктуру, блокирование систем онлайн-торговли, геоинформационных систем и хакерские атаки на сайты компаний
Государство	Атаки на ключевые государственные системы управления (электронное правительство, сайты государственных структур), экономическая блокада (масштабное отключение платежных систем, систем бронирования), аппаратные атаки на персональные компьютеры и критически важную инфраструктуру государственных предприятий

Киберпреступники используют свой арсенал информационного оружия, представляющий собой совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения. К основным видам информационного оружия относят следующие:

- бэкдор (backdoor, от англ. back door - черный ход). Данный инструмент предполагает скрытый метод в системе, который позволяет получить доступ к защищенной области;

- компьютерные "вирусы" - специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, "вирусы" способны самостоятельно размножаться[3];

- "логические бомбы" - программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

- программные продукты типа "троянский конь" - программы или утилиты, которые после установки выполняет незаявленные функции в фоновом режиме;

- нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения;

- анализаторы трафика (sniffer) - программы или устройства, которые контролируют данные, передаваемые по сети. Традиционно используемые для законных функций сетевого управления, они могут применяться и во время кибератак с целью кражи информации;

- DDos-атаки - предназначены для нарушения доступа к сети, как правило, при помощи выполнения миллионов запросов каждую секунду, в результате чего доступ к сети затрудняется или нарушается;

- E-mail Spoofing - это метод отправки электронной почты с подменой источника, используется для того, чтобы заставить получателя предоставить конфиденциальную информацию;

- Keylogger - представляет собой программное или аппаратное средство, предназначенное для контроля нажатия клавиш на клавиатуре компьютера, для получения пароля, пин-кода или другой информации[4].

Компанией Group-IB при участии экспертов центра реагирования на компьютерные инциденты CERT-GIF было проведено исследование состояния и динамики развития современного рынка компьютерных преступлений и актуальных киберугроз за 2012 г. По результатам проведенного анализа были определены оценки объема различных сегментов рынка киберпреступности, в которую вовлечены русскоговорящие преступные группы (рис. 1-3)[5].

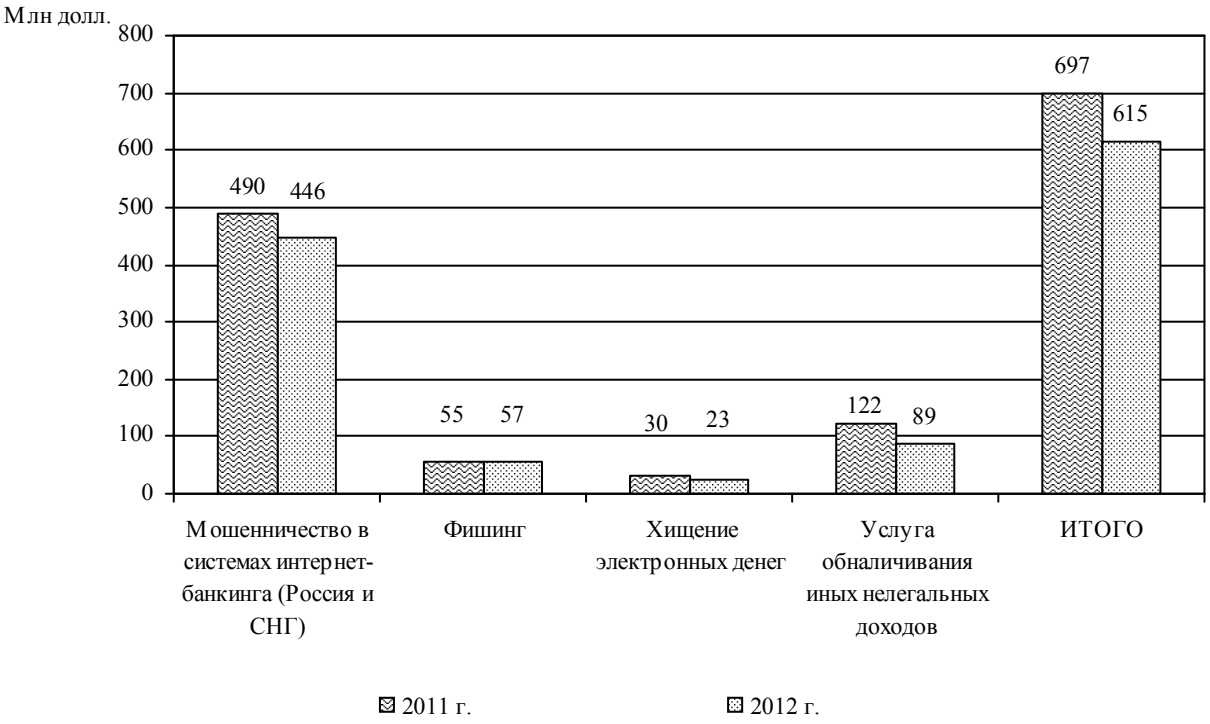

Рис. 1. **Оценка объема сектора "Интернет-мошенничество"**

Источник. Рассчитано на основании данных компании Group-IB.

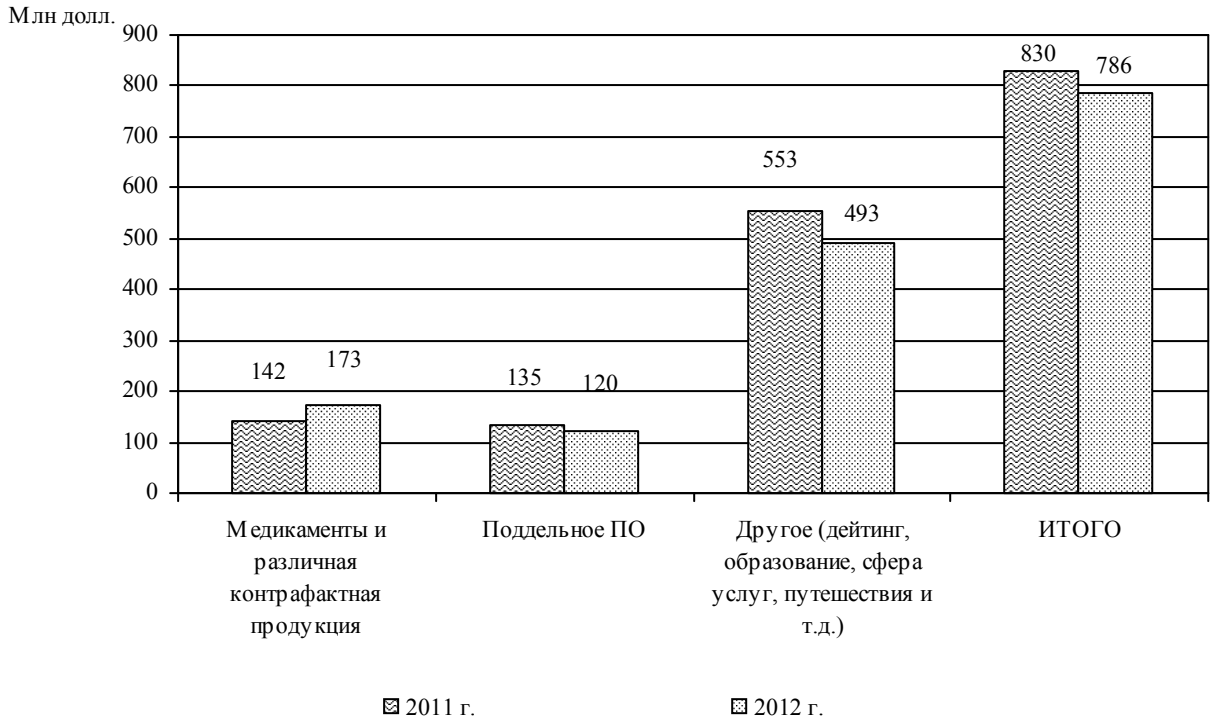

Рис. 2. **Оценка объема сектора "Спам"**

Источник. Рассчитано на основании данных компании Group-IB.

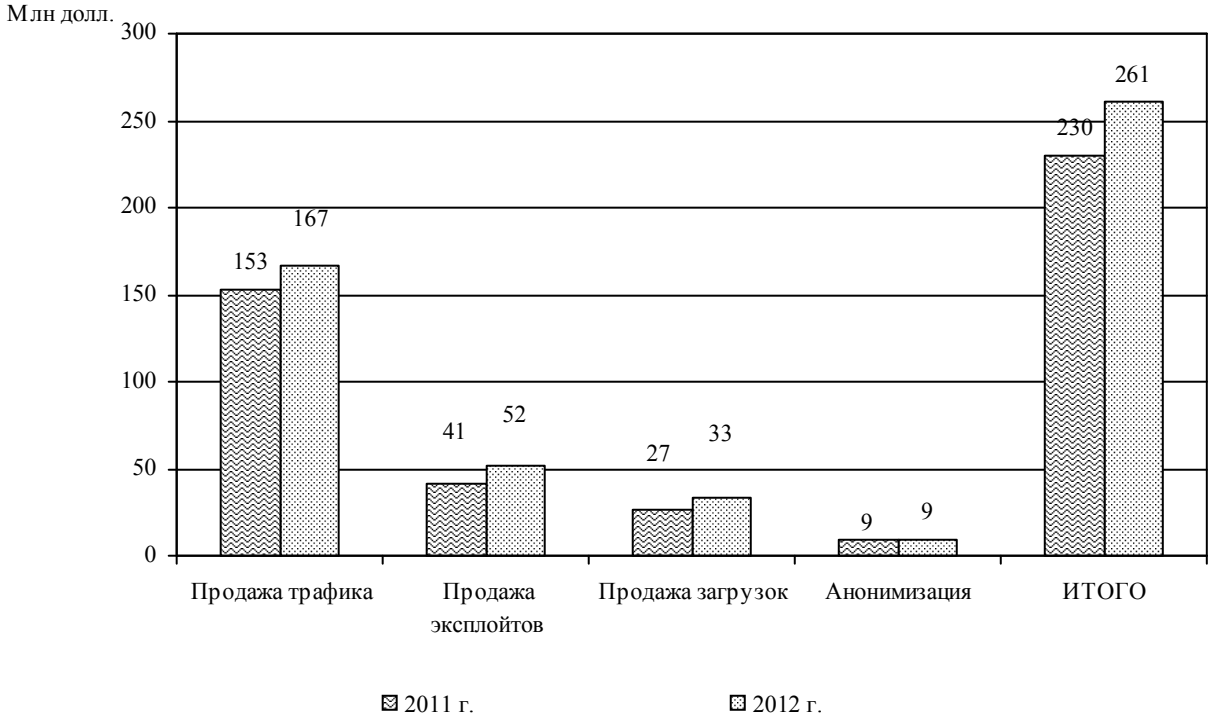

Рис. 3. **Оценка объема внутреннего рынка (C2C)**

Источник. Рассчитано на основании данных компании Group-IB.

В 2012 г. средняя сумма хищений с банковского счета юридических лиц составила 1 641 000 руб., физических лиц - 75 000 руб.

В 2012 г. рост объемов продаж различной контрафактной продукции через спам-рассылки составил 22 %.

Рост внутреннего C2C-рынка составил 13 %. Причиной тому является увеличение расходов на организацию бот-сетей и распространение вредоносного программного обеспечения, что вызвано общим ростом защищенности клиентских рабочих станций и развитием используемого программного обеспечения.

Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор времени и места применения, наконец, экономичность, делают информационное оружие чрезвычайно опасным: оно легко маскируется под средства защиты, скажем, интеллектуальной собственности, но позволяет при этом очень эффективно проводить акты информационного терроризма.

Состояние киберпреступности в стране позволяет выделить ряд устойчивых тенденций. Большинство случаев неправомерного доступа к компьютерной информации, составляющих на сегодня 19 % от общего числа зарегистрированных компьютерных преступлений, или изготовления вредоносного программного обеспечения (8 %) направлено на хищение денежных средств. Число преступлений, совершаемых из хулиганских побуждений, крайне незначительно. Преступники-одиночки постепенно вытесняются с криминального рынка преступными группами, объединяющими людей из разных регионов России или стран мира[6].

Высокий уровень киберпреступности в стране, темпы развития информационных технологий вызывают необходимость увеличения затрат на информационную безопасность. По результатам аналитического исследования, проведенного компанией “Код безопасности”, в 2013 г. государственные ведомства потратили на защиту информационных ресурсов около 4,8 % своих ИТ-бюджетов[7].

Таким образом, естественными причинами возникновения, существования и увеличения числа киберпреступлений являются совершенствование информационных технологий, расширение производства поддерживающих их технических средств и сферы их применения, возможность виртуальных форм расчетов как потенциальный объект преступного посягательства и все большая доступность подобных устройств.

Общественная опасность подобных преступлений заключается в их латентности, которая, в свою очередь, образуется в результате того, что потерпевший зачастую и не понимает, что в отношении него совершено преступление, что дает злоумышленнику уверенность в своей безнаказанности.

Высокая социальная опасность киберпреступности объясняется ее транснациональным и организованным характером, поэтому ни одно государство сегодня не способно активно противодействовать этой угрозе самостоятельно, в связи с чем неотложной является потребность активизации международного сотрудничества.

Эффективная борьба с киберпреступностью требует коллективных усилий. Для этого необходимо вести постоянную разъяснительную работу среди населения. Требуется длительный и, что немаловажно, упорный воспитательный процесс для того, чтобы люди осознавали необходимость мер предосторожности.

Для того чтобы эффективно противостоять киберпреступности, масштабы которой столь разительно выросли за последние годы, государственным структурам и коммерческим компаниям необходимо рассматривать информационную безопасность в качестве одного из ключевых компонентов своей деятельности. Наиболее приоритетными должны стать вопросы ответственности, соблюдения российского законодательства в области информационной безопасности и повышения уровня культуры безопасности граждан.

---

[1] Сайт министерства внутренних дел Российской Федерации. URL: http://mvd.ru.

[2] Norton report 2013: аналитический. отчет URL: http://www.symantec.com/about/news/resources/press_kits/ detail.jsp?pkid=norton-report-2013.

[3] Сайт компании “Лаборатория Касперского”. URL: http://www.kaspersky.ru.

[4] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism // Threats For Leavenworth. 2005. 15 August. URL: http://handle.dtic.mil/100.2/ADA439217.

[5] Group-IB Total intelligence report 2012-2013. URL: http://report2013.group-ib.com.

[6] *Мошков А.Н.* Киберпреступность усиливает свои позиции. URL: http://www.securitylab.ru/ blog/company/Personal_data/an-moshkov-kiberprestupnost-usilivaet-svoi-pozitsii .php.

[7] Сайт компании “Код безопасности”. URL: http://www.securitycode.ru.

Поступила в редакцию 02.07.2014 г.