

Чернова Мария Алексеевна

студентка

Лошкарев Андрей Викторович

доцент

ФГБОУ ВО «Самарский государственный

экономический университет»

г. Самара, Самарская область

КИБЕРПРЕСТУПНОСТЬ КАК РАЗВИВАЮЩАЯСЯ КРИМИНАЛЬНАЯ УГРОЗА ОБЩЕСТВУ

***Аннотация:** в данной статье рассматривается киберпреступность – одна из самых новых криминальных угроз обществу. Эта сфера преступлений развивается достаточно быстро и уже успела нанести значительный вред обществу. Одной из основных проблем борьбы с киберпреступлениями является то, что в нашей стране слабо развиты законодательство в сфере информационных преступлений и методики борьбы с ними.*

***Ключевые слова:** киберпреступность, киберпреступления, компьютерная криминалистика, кибербезопасность.*

Киберпреступления в России и во всем мире имеют быструю динамику развития. Киберпреступление – это «преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей»-по мнению, В.А. Номоконова и Т.Л. Тропина [1]. Количество киберпреступлений и число пострадавших от действий хакеров постоянно увеличивается. Но государства и общество не выработало эффективных мер борьбы против такого вида преступлений.

Рост количества киберпреступлений связан с тем, что в современном обществе огромную роль играет интернет и вся информация хранится в электронном виде. Также сейчас все большее распространение получили электронные деньги, которые больше всего подвергаются нападкам хакеров. Кроме этого киберпре-

ступники работают на заказ – сформировался устойчивый спрос на услуги киберпреступников. Наиболее часто встречающаяся услуга на рынке киберпреступлений – неправомерный доступ к личной информации (аккаунты в социальных сетях, электронные почты).

Понятие «компьютерная криминалистика» только зарождается в России, применяемые методы расследования компьютерных преступлений имеют малое распространение, судебные экспертизы проводятся по методикам, которые получили еще мало научного обоснования и практического применения.

С каждым годом количество киберпреступлений растет. Так в 2014 году МВД России зарегистрировало 11 000 компьютерных преступлений. По словам Мошкова, на долю краж и мошенничеств в 2014 году пришелся 41% киберпреступлений (в 2013 году этот показатель составлял 30%). При этом официальная статистика учитывает только поданные заявления от потерпевших. А значит количество киберпреступлений совершается еще больше [2].

Отмечается постоянный рост числа киберпреступлений в финансовых и банковских сферах. Так, ущерб экономике России от киберпреступности в 2015 году составил 0,25% от ВВП или 203,3 миллиарда рублей, а затраты на ликвидацию последствий – более 79,8 миллиарда рублей. Более 92% крупных коммерческих компаний, госструктур, а также предприятий малого и среднего бизнеса столкнулись с киберинцидентами. Прямой финансовый ущерб составил 123,5 миллиарда рублей.

Глава Кибернетического командования США, директор Агентства национальной безопасности и руководитель Центральной службы безопасности адмирал Майкл Роджерс включил Россию в список основных угроз в киберпространстве: «В России находятся достаточно мощные киберсилы, способные действовать с высокой скоростью и точностью, оставаясь в тени. В России также живут одни из самых профессиональных кибермошенников в мире, жертвы которых есть во всем мире», – заявил Роджерс [2].

Согласно немецкой IT-компании Deutsche Telekom, Россия по совершаемым кибератакам занимает 4 место, уступая Вьетнаму, США и Китаю. В 2013 году

количество кибератак России составило 2,5 млн, а на сегодняшний день их насчитывается почти 7 млн, т.е. за три года их количество возросло в 2,8 раза [3].

Для эффективного предотвращения киберпреступлений необходим целый ряд мер, направленных как на предупреждение, так и на пресечение действий злоумышленников. Среди мер общепрофилактического характера преступлений в сфере компьютерной информации в качестве сдерживающего фактора нередко называют ужесточение уголовного законодательства.

В действующем УК РФ есть только одна глава, которая предусматривает ответственность за киберпреступления – глава 28 «Преступления в сфере компьютерной информации», в которой содержится всего 3 статьи (272, 273, 274) [3]. В примечании к ст. 272 УК РФ сказано, что под компьютерной информацией понимаются сведения (сообщения, данные) представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Верховный Суд РФ изложил свое мнение на данное примечание в абз. 29 официального отзыва от 7 апреля 2011 г. «На проект федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации»: «Предложенный в примечании термин «электрические сигналы», на наш взгляд, не вносит достаточной ясности и требует дополнительного пояснения». Так как, компьютерные сети используют для передачи данных оптоволокно, в котором сведения передаются с помощью переноса света, а не электрических сигналов.

Статьей 272 УК РФ предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло за собой ее уничтожение, блокирование, модификацию либо копирование. Следует отметить, что физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся на нем, не влечет за собой последствий, предусмотренных ст. 272 УК РФ, поскольку объектом преступного посягательства является компьютерная информация, а не носитель.

Аналогичные проблемы, связанные с наличием устаревшего определения компьютерной информации и отсутствием четких определений уничтожения,

блокирования, копирования компьютерной информации, возникают и при применении ст.ст.273–274 УК РФ. Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, но на практике практически не используется.

29 ноября 2012 г. был принят Федеральный закон №207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», который впервые в российском законодательстве выделил различные виды мошенничества в отдельные составы преступлений в зависимости от того, в какой сфере они совершены. Благодаря данному закону появились ст. 159.3 УК РФ «Мошенничество с использованием платежных карт» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» [5].

Кроме слабой нормативно-правовой базы в сфере компьютерной криминалистики, существует еще одна проблема предотвращения киберпреступлений и наказаний за них – это неготовность правоохранителей расследовать такие категории дел, в частности из-за отсутствия терминологического аппарата. В правоохранительных органах нет специалистов, которые могли бы предотвратить преступления хакеров.

Таким образом, общественная опасность киберпреступлений еще не в полной мере осознана законодательством. Несоразмерность нанесенного вреда и наказания за этот вред очевидны. Даже несмотря на то, что в законодательстве УК РФ были сделаны незначительные поправки в сфере компьютерной криминалистики, не делает наше законодательство в этой сфере совершенным, проблемы в определении правильного наказания остаются актуальными. Киберпреступники в России не приравниваются к обычным и за преступления такого рода ответственность ниже. Украдший большую сумму денег киберпреступник зачастую может отделаться условным сроком. В то же время, если бы та же сумма была украдена традиционным способом, то преступника ждало бы лишение свободы на 10–15 лет – считают эксперты [6].

Список литературы

1. Номокова В.А. Киберпреступность как новая криминальная угроза / В.А. Номокова, Т.Л. Тропина. – 2012.
2. Киберпреступность и киберконфликты: Россия [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберкон
3. Показатели кибератак [Электронный ресурс]. – Режим доступа: <http://www.sicherheitstacho.eu/#>
4. Уголовный кодекс РФ от 13.06.1996 №63 – ФЗ.
5. Алина Михайлова, Проблемы кибербезопасности в России и пути их решения [Электронный ресурс]. – Режим доступа: <http://www.garant.ru/article/520694/#sdfootnote1sym>
6. Кантышев Павел. МВД зарегистрировало около 11 000 киберпреступлений в 2014 г. [Электронный ресурс]. – Режим доступа: <http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya>