законодавства. А сутність будь-якого галузевого законодавства багато в чому визначають обставини, які характеризують стан суспільних відносин, напрямки і динаміку їх розвитку, необхідність правового закріплення їх тенденцій, у тому числі і охорони тих, які держава вважає за необхідне.

Існуючі у вітчизняному кримінальному праві тенденції щодо імплементації норм міжнародного права, а також окремих положень кримінального права країн, які здійснюють ефективну протидію окремим видам злочинів (зокрема, господарським, корупційним), є позитивними й такими, що заслуговують на підтримку. Але при цьому, на жаль, якість законопроектів, за допомогою яких здійснюються такі зміни, у переважній більшості випадків є вкрай низькою. Аналіз показує, що при їх підготовці досить часто ігноруються правила законодавчої техніки, системність кримінального законодавства, фактично руйнуються основоположні засади і принципи, вироблені не лише вітчизняною наукою кримінального права, а й визнані у всьому цивілізованому світі.

Таким чином, проаналізувавши вищевикладене, вважаємо, що наступність у кримінальному праві має дійсно важливе значення для подальшого його розвитку, адже наступність у праві в найзагальнішому вигляді означає використання попереднього правового досвіду з метою подальшого реформування. Такий досвід може бути використаний у правотворчості, у правозастосовній практиці, у науці, у системі юридичної освіти і навіть під час викладання конкретних юридичних дисциплін.

УДК. 343. 79

Оксана Александровна ШУТ,
старший преподаватель кафедры правовых дисциплин Северо-Казахстанского Государственного Университета имени Манаша Козыбаева

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

В 21 веке среди бесчисленных разновидностей преступлений широкое распространение получила информационная преступность. Считается, что преступления, которые совершаются с использованием информационных технологий в преступных целях, называются преступления «киберпреступность».

В. В. Крылов дает следующее определение информационных преступлений: «это общественно опасное деяние, запрещенное уголовным законом под угрозой наказания, совершенные в области информационных правоотношений». Информационные правоотношения он определяет как отношения, возникшие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска информации, прав субъектов, участвующих в информационном процессе и информатизации. Данное определение было одной из первых попыток определить понятие информационных преступлений, потому, не удивительно, что оно имеет очень широкое понятие, а также, внимание автора было сосредоточено лишь на компьютерных преступлениях (1, с. 186).

А. В. Суслопаров дает свое определение данному понятию: «Информационными преступлениями являются общественно опасные

противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности, способом совершения которых является информационное воздействие или (и) предметом которого является информация как особый нематериальный объект». Данное же определение также имеет свои изъяны, такие, как квалификация предмета. В правовой культуре принято считать предмет преступления объектом материального мира (2, с. 31).

Таким образом, установлено, что в попытках дать определение информационным преступлениям, к общепринятому определению современные ученые так и не пришли. Но всё же, большинство сошлось во мнении, что неотъемлемым элементом информационных преступлений является «информация».

Главное свойство информации состоит в том, что любая передача информации по факту является ее копированием. Данное свойство информации делает любые аналогии, связывающие информационное действие и отношение по поводу материальных объектов, неправомерными. Информацию невозможно украсть, в ее отношении не действуют стандартные гражданско-правовые отношения купли-продажи и другие. Перемещение информации представляет собой копирование информации и последующее уничтожение её у предыдущего субъекта.

Можно выделить следующие признаки информации: самостоятельные сведения, многократность использования, возможность математического анализа, системность и другие. Из данного перечня наиболее значительным будет являться сохранение информации у передающего и принимающего субъекта.

Так как информация не является материей в привычном ее понимании, то логично, что информация не материальна. Такое понимание информации наталкивает на следующие следствия. Нематериальные объекты не имеют возможность существовать самостоятельно, так как для их восприятия необходим материальный субъект, выступающий носителем. К материальным носителям информации относят следующие объекты: бумага, компакт-диск, флэш-накопитель, волны (электромагнитные, звуковые, световые). Помимо этого, стоит отметить и мозг человека как материальный носитель информации (3, с. 285).

Поэтому предметом преступления может быть признано лишь то, что: а) не совпадает с объектом преступления (общественными отношениями), б) непосредственно выражает в себе свойства данного объекта, в) позволяет путем воздействия на него причинить вред объекту преступления (4, с. 62).

Исходя из этого и из свойств информации, в качестве предмета (или скорее квазипредмета) преступления ее можно рассматривать только при наличии ее непосредственной связи с объектом посягательства и при условии, что именно информационное воздействие причиняет вред объекту уголовно-правовой охраны.

В перечень преступлений в сфере информационных технологий входят такие преступления как: распространение вредоносных вирусов, взлом паролей, кража номеров кредитных карт, распространение запрещенной информации или товара (наркотики, порнография, материалы, возбуждающие межнациональную или межрелигиозную вражду) в интернете (5, с. 144).

Помимо этого, в число распространённых и наиболее опасных преступлений, совершаемых с использованием интернета, входит мошенничество. Опасность таят такие денежные транзакции, как инвестирование денежных средств на иностранные фондовые рыки с использованием сети Интернет, что имеет огромный риск быть вовлеченным в различные мошеннические схемы. Другой пример, Интернет-аукционы, на которых сами продавцы делают ставки на товар, тем самым повышая стоимость выставленного на аукцион товара (6).

Особую угрозу представляют преступления: распространение вредоносных программ, нарушающие деятельность автоматизированных систем управления и контроль различных объектов, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, и повлекут не только имущественный ущерб, но и могут причинить физический вред.

В законодательстве Республики Казахстан ещё в середине 90-х были прописаны нормы, предусматривающие уголовное наказание за преступления в информационных сетях. Но то было в эпоху разгара нового преступного течения, сейчас же количество данных норм существенно увеличилось, а современные сетевые преступники стали намного профессиональней. Если раньше обычный «хакинг» был широко распространен среди амбициозных хакеров одиночек-энтузиастов, то ныне в мире действуют крупные организованные преступные группировки, чья деятельность имеет одну корыстную цель – заработать денежные средства преступным путем. Для своей успешной работы хакеры используют «бот-неты», это крупные сети из сотни, тысячи, а то и сотни тысяч компьютеров, разбросанных по всему миру, контроль над которыми установили «хозяева» бот-нета, занимающиеся определенной деятельностью, такими как: подбор паролей, рассылка рекламных сообщений, атаки на компьютерные базы данных (7, с. 69).

Широкое распространение компьютеров и интернета в современном обществе, а также совершенствование инструментов для несанкционированного доступа к личной информации привело к тому, что для совершения сетевого преступления не требуется специальное образование. Приобрести такой навык может практически каждый пользователь, самостоятельно освоив лишь несколько «хакерских» приемов.

Все чаще объектом сетевых преступлений является авторское право, права и свободы человека, интересы государства. Также встречаются ситуации, где используются информационные технологии для осуществления диверсий (8, с. 503).

Большинство информационных преступлений можно избежать, если соблюдать простые правила безопасности в сети, а также использовать разного рода профилактические мероприятия. Данные действия следует понимать, как деятельность, направленную на обнаружение и устранение причин, возбудившие преступления, и условия, способствующие их совершению. Для борьбы с информационной преступностью можно выделить несколько основных групп мер предупреждения информационных преступлений:

- правовые;

- организационно-технологические;

- криминалистические.

Таким образом, можно сделать вывод, что неоднозначная квалификация, сложность компьютерной техники и информационных технологий, а также трудность сбора доказательственной информации, не приводит к достаточному количеству раскрытых преступлений. К большому сожалению, даже имея достаточно полный набор элементов портрета преступника, это дает лишь 30-40 % информации по конкретному преступнику. Любое исполненное высокотехничное преступление остается нераскрытым, если преступники не совершили серьезных ошибок или, кто-то из преступников не решил сознаться в преступлении, изобличив подельников (9, с. 72).

Однако криминологическая характеристика даёт возможность в какой-то степени предвидеть, что может принести конкретное правонарушение с точки зрения личности преступника и его действий, на что следует обратить внимание, какие меры можно планировать и какую реакцию стоит ожидать больше всего от преступника (10, с. 256). А это уже что-то, по крайней мере, данные техники помогут изобличить неопытных преступников или матерых хакеров, допустивших ошибки в своей преступной деятельности. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И мировые специалисты-криминалисты внесут достаточный вклад для решения данной проблемы.

Список библиографических ссылок:

1. Гребеньков А. А. Преступность в сфере высоких технологий: исторический аспект. *Известия Юго-Западного государственного университета*. Серия «История и право». 2012. № 1-1. С. 184-188.

2. Суслопаров А. В. Информационные преступления: автореф. дис. канд. юрид. наук. Красноярск, 2008. С. 184.

3. Хананашвили М. М. «Информационные неврозы». Ленинград, 1992. С. 350.

4. Числин В. П.Информация как объект уголовно-правовой защиты. М.: Макс Пресс, 2004. С. 127.

5. Крылов В. В. Основы криминологической теории расследования преступлений в сфере информации. М.: МГУ, 1998. С. 250.

6. Голубев В. А., Головин А. Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий. URL: http:// crime-research. org /articles.

7. Полный курс уголовного права: в 5 т. / под ред А. И. Коробеева. СПб.: Юридический центр Пресс, 2008. Т. 2: Преступления против личности. С. 682.

8. Рассолов М. М. Управление, информация, право. М.: Мысль, 1983. С. 157.

9. Мешков В. М., Григорьев А. Н., Проценко Н. Ю. Компьютерные преступления и защита компьютерной информации. Калининград, 2003. С. 120.

10. Белкин Р. С. Криминалистическая энцеклопедия. М.: Бек, 1997. С. 342.