УДК 343.13

Э.Л. Кочкина

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «КИБЕРПРЕСТУПЛЕНИЕ». ОТДЕЛЬНЫЕ ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ

В статье рассматривается актуальность киберпреступлений, их виды и возможные способы их совершения, особенности киберпреступлений. Предлагаются соответствующие меры профилактического характера. Приведены точки зрения различных авторов, относительно определения понятия «киберпреступление».

Ключевые слова: кибероружие, киберпреступление, киберпространство, киберпреследование, киберпорнография, кибертерроризм, социальная инженерия, фарминг, финансовые преступления, фишинг.

E.L. Kochkina

DEFINITION OF THE CONCEPT «CYBERCRIME». SELECTED TYPES OF CYBERCRIME

The article examines the relevance of cybercrime, their types and possible ways of their fulfillment, the peculiarities of cybercrime. Proposed preventive measures are proposed. The points of view of various authors are given regarding the definition of the concept «Cybercrime».

Keywords: cyber-weapons, cybercrime, cyber-space, cyber-crime, cyber-pornography, cyber-terrorism, social engineering, farming, financial crimes, phishing.

Активный рост всевозможных киберугроз в современном обществе ставит перед каждым государством чрезвычайно актуальную задачу – необходимость обеспечение информационной безопасности. Мировая ежегодная оценка состояния данного вида преступности, вызывает опасения в связи с низким уровнем защищенности граждан современного информационного общества, при этом спектр проблем достаточно широк – от технической незащищенности до уязвимости систем обеспечения работы, предназначенных для проведения операций с денежными средствами. Не смотря на то, что изучение данной проблемы ведется не одно десятилетие, тем не менее не достаточно полно сформировано понятия наказания, что позволяет широко «разворачи-

ваться» преступным сообществам. До сих пор в Уголовном кодексе РФ нет определения «киберпреступление». В современной юридической литературе под «киберпреступлениями» понимают «преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами», «преступления в высоких компьютерных технологиях», «преступления в информационном пространстве» и т.д. Многие ученые и исследователи предприняли попытку определить данное понятие. По мнению, В.А. Номоконова, Т.Л. Тропиной киберпреступление является более обширным, чем компьютерная преступность и точно отражает такое явления, как преступность в информационном пространстве [1]. Нужно отметить, что киберпространство (от англ.cyberspace) – это пространство, которое симулируется и опосредствуется электронными устройствами [2]. На наш взгляд наиболее полное определение, отражающее аспекты данного негативного явления дается в статье Д.Н. Карпова «киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба, индивиду, организации или государству посредствам любого технического средства с доступом в Интернет». По большому счету отражаются не юридические аспекты, а имеющие социально-экономические проблемы современного общества. К.Н. Евдокимов дает несколько определений понятию «Компьютерная преступность», ссылаясь на различные мнения отечественных авторов [3]. При этом, указывает, что компьютерную преступность целесообразно рассматривать в узком и широком смыслах.

В узком смысле «компьютерная преступность» представляет собой совокупность преступлений, где в качестве непосредственного основного объекта преступного посягательства выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом преступления являются компьютерная информация, средства защиты компьютерной информации, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации». Данное определение, по их мнению, полностью совпадает с установленным законодателем понятием «преступления в сфере компьютерной информации». В широком смысле определению «компьютерная преступность» дается следующая трактовка: «компьютерная преступность представляет собой совокупность преступлений, где ос-

новным непосредственным объектом преступного посягательства выступают общественные отношения в сфере компьютерной информации и информационных технологий, безопасного функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, но при этом компьютерная информация, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, смартфоны, айфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства) являются не только предметами преступного деяния, но и используются в качестве средства и орудия совершения преступления. В Конвенции о киберпреступности, открытой для подписания в г. Будапеште, вступившей в силу 1 июля 2004 г. киберпреступлениями являются деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а так же злоупотребления такими системами, сетями и данными [4]. Согласно данным, представленным институтом судебных экспертиз и криминалистики в период с апреля 2015 г. по март 2016 г. со счетов российских банков злоумышленниками было украдено 348,6 млн р. по сравнению с аналогичным интервалом 2014–2015 гг., похищенная сумма возросла в 5 раз[1]. Это говорит о том, что данный вид преступлений способен стремительно расти. Способы и методы совершения преступлений идут «в ногу» со способами защиты компьютерной информации, а в большинстве случаев вообще впереди. Российское информационное агентство сообщает, что в 2016 г. с банковских карт, принадлежащих жителям России, злоумышленники похитили порядка 650 млн р. Во всех случаях преступники пользовались методами социальной инженерии. А уже по итогам первого полугодия 2017 г. было похищено 550 млн р., поэтому есть все основания считать, что к концу года рекорды будут побиты[2].

По мнению авторов книги «Социальная инженерия и социальные хакеры» М.В. Кузнецова, И.В. Симдянова, социальная инженерия – это манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации [5]. Как отме-

[1] Кибермошенники за год украли со счетов россиян почти 350 млн р. [Электронный ресурс] // Общая газета : офиц. сайт. URL: http://og.ru/society/2016/10/13/84213.

[2] С банковских счетов россиян украли 650 млн р. [Электронный ресурс] // URA.RU : офиц. сайт. URL: https://ura.news/1052300513.

чают, данные авторы, самую большую угрозу информационной безопасности будут представлять, все более совершенствующиеся методы социальной инженерии, применяемые для взлома существующих средств защиты. Объясняя это тем, что социальная инженерия не требует значительных финансовых вложений и досконального знания компьютерных технологий злоумышленниками. Эту точку зрения разделяют Рич Могулл глава отдела информационной безопасности корпорации Gartner и Роб Форсайт, управляющий директор одного из региональных подразделений антивирусной компании Sophos, который характеризует его как «новый циничный вид мошенничества».

Рассмотрим некоторые виды киберпреступлений.

Финансовые преступления – общественно опасные деяния, посягающие на финансово-экономические отношения, а именно мошенничество с кредитными картами, хищение денежных средств в момент совершения банковских операций и т.д.

Фишинг – это выведывание информации у доверчивых граждан для доступа к банковским счетам. Распространен в государствах, где популярны услуги интернет-банкинга. На сегодняшний день получил свое распространение целевой фишинг.

Целевой фишинг используется на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальных жертв открыть исполняемый файл или перейти на сайт содержащий вредоносный код. Более опасным видом мошенничества, чем фишинг, является так называемый фарминг. Фарминг – это процедура скрытного перенаправления жертвы на ложный IP-адрес. На наш взгляд является более изощренный, хотя и технически сложный метод мошенничества, чем фишинг. Так же опасным видом киберпреступления является удаленный взлом компьютеров, за счет которого злоумышленники имеют возможность читать и редактировать документы, которые сохраняются на файл-серверах и на рабочих столах компьютеров, имеют возможность внедрять собственные вредоносные программы, а также собирать различного рода информацию, посредством аудио, видео наблюдения. Один из новейших вирусов, появившихся в последнее время стало кибероружие, целью которого является уничтожение промышленной инфраструктуры. К ним относятся такие вирусы как Duqu, Stuxnet, Gauss, Flame. За подобными вирусами стоят уже не низкоквалифицированные специалисты информационных технологий, а очень суперпрофессионалы.

Информационный сайт «Человек и прогресс»[1], посвященный влиянию научно-технического прогресса на личность, приводит некоторые виды киберпреступлений:

«Кибер-порнография – относятся порнографические сайты, разрешающие посетителям размещать порнографические фильмы, видеозаписи и фотографии с несовершеннолетними гражданами.

На наш взгляд, будет справедливо отнести так же чаты знакомств, содержащие порнографическую информацию о пользователях и описание виртуального секса с несовершеннолетними гражданами.

Кибер-торговля наркотиками – это наркоторговля с использованием новейших технологий шифрования сообщений, передаваемых клиентами по электронной почте. В таких сообщениях наркоторговцы указывают в кодированном виде место и способ осуществления обмена товара на денежные средства.

Кибертерроризм – это совершение террористических актов в киберпространстве. К этой категории преступлений может относится простое распространение через Интернет информации о терактах, которые могут быть совершены в будущем в конкретно указанное время.

А также выделяют такие виды киберпреступлений, как азартные игры-онлайн и киберпреследование.

Нужно отметить, что жертвами киберпреступлений становятся несовершеннолетние граждане. Согласно информации следственного комитета Российской Федерации по Иркутской области самым страшным и необратимым процессом воздействия на детей стало массовое вовлечение их в суицидальные группы, в которых романтизируется смерть, популяризуется уход из жизни[2]. Воздействовать на ребенка могут не только путем прямого контакта в переписке в социальных сетях, но и через предложения просмотра видео, обсуждение сериалов, в помощи решения домашнего задания. Также могут предлагаться определенные онлайн-книги, рекомендации по прочтению литературы и прослушивание музыки.

Одним из ярких примеров современного времени является интернет-игра для детей и подростков «Синий кит», финальный этап кото-

---

[1] Проблема киберпреступности [Электронный ресурс] // Человек и прогресс: офиц. сайт. URL: ultraprogress.ru/problema-kiberprestupnosti.html.

[2] Спасение детей от киберпреступлений [Электронный ресурс] // Следственное управление следственного комитета Российской Федерации по Иркутской области : офиц. сайт. URL: irk.sledkom.ru/folder/1076968.

рой является суицид участника. В начале 2017 г. информационный сайт «Известия» опубликовал статью «Возращение «Синего кита», в которой привели статистические данные. По указанной информации в участии указанной игры подозревалось 130 детей, погибших по разным обстоятельствам с 2015 по 2016 г. Так же приводится список заданий для участников, таких как, порезать губу, такать руки иголкой, сидеть вниз ногами на краю крыши, рисовать на руках и ногах лезвием и т.д.

Такие страны, как Россия, Украина, Болгария, Латвия, Италия, Ближний Восток, США уже «столкнулись» с «Синим китом». На сегодняшний день активно ведется борьба с данным видом преступления.

Сегодня активно ведутся профилактические меры по предупреждению подобных киберпреступлений, жертвами которых становятся несовершеннолетние граждане. К примеру, следственный комитет Российской Федерации по Иркутской области предложил памятку для родителей о спасении детей от киберпреступлений.

Из этого следует, что киберпреступления подрывают не только компьютерную безопасность общества, информационную безопасность пользователей ЭВМ, но и общественный порядок государства в целом. В результате приведенных в статье определений «киберпреступлений», а так же отдельных видов данной категории преступлений можно сформулировать общее определение. Киберпреступление – это совокупность преступлений, запрещенных Уголовным кодексом РФ, совершаемых в киберпространстве, где основными непосредственными объектами преступного посягательства выступают:

– конституционные права и свободы человека и гражданина;

– общественные отношения в сфере компьютерной информации и информационных технологий;

– общественные отношения в сфере экономики и экономической деятельности;

– общественные отношения в сфере государственной власти;

– общественные отношения в сфере здоровья населения и общественной нравственности.

Преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, злоупотребление этими системами, сетями и данными. Это нарушение охраняемых законом общественных отношений в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, с целью нанесения экономического, политиче-

ского, морального, идеологического, культурного и других видов ущерба человеку, обществу, государству и миру в целом.

Определяются особенности киберпреступлений, к которым относят: трансграничность; нестандартность способов совершения; автоматизация преступных деяний; анонимность деяний; сложность раскрываемости данного вида преступлений (низкий процент раскрываемости); взаимодействие различных преступных сообществ; высокие доходы преступной деятельности.

Нужно отметить, что киберпреступления охватывают широчайший пласт общественных отношений, имеют большое количество разнообразных способов совершение данного вида преступления. Данный вид преступлений подрывает не только информационную безопасность общества, но и общественный порядок всего государства, который включает в себя лишении материального плана, но и угрозу жизни и здоровья граждан. Борьба с киберпреступлениями должна осуществляться на международном уровне. Для эффективного раскрытия данного вида преступлений необходимо активное международное сотрудничество взаимопомощь и поддержка, а так же постоянное обновление межгосударственных, внутригосударственных законов. Но также нужно отметить, что для большего успеха каждому государству необходимо принимать внутригосударственные законы, которые не должны противоречить друг другу. Как отмечает, К.Н. Евдокимов правовое регулирование вопросов борьбы с киберпреступлениями является базисом всей системы противодействия киберпреступности, соответственно изменения и дополнения в действующее уголовное законодательство необходимо и актуально на современном этапе развития общества. Киберпреступления, несомненно, попадают под юрисдикцию Уголовного кодекса РФ, согласно которому существует перечень статей, по которым привлекают к ответственности преступников, а именно:

– ст. 146 УК РФ. Нарушение авторских и смежных прав;

– ст. 159 УК РФ. Мошенничество;

– ст. 242 УК РФ. Незаконные изготовление и оборот порнографических материалов или предметов;

– ст. 272 УК РФ. Неправомерный доступ к компьютерной информации;

– ст. 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ;

– ст. 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

Анализируя выше приведенные виды киберпреступлений становится очевидным необходимость их предупреждения. Иногда совершение даже не очень серьезного преступления может привести к опасным последствиям, которые быть могут и непоправимыми. Законодателю целесообразнее было бы принять меры ужесточению санкций статей отдельных составов уголовно наказуемых преступных деяний, имеющих отношение к киберпреступлениям.

Список использованной литературы

1. Номоконов В.А. Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология. Вчера. Сегодня. Завтра. – 2012. – №1 (24). – С. 47.

2. Аберкромби Н. Социологический словарь [Электронный ресурс] / Н. Аберкромби, С. Хилл, Б.С. Тернер. – URL: http://sociological_dictionary.academic.ru/264.

3. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова.– М., 2016.

4. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М., 2002.

5. Кузнецов М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб., 2007.

Информация об авторе

Кочкина Эльвира Леонидовна – магистрант, Российский государственный университет правосудия, Восточно-Сибирский филиал, 664074, Российская Федерация, г. Иркутск, ул. Ивана Франко, 23а, e-mail: elvira.kostina@list.ru.

Information about the author

Kochkina, Elvira L. – Masters Degree Student, Russian State University of Justice, East Siberian Branch, 23a, Ivan Franko st., 664074, Irkutsk, Russian Federation, e-mail: elvira.kostina@list.ru.