УДК 343.9

Карпенко Людмила Константиновна,
кандидат юридических наук, доцент,
Донецкий национальный университет,
г. Донецк, Донецкая Народная Республика
orion09052019@mail.ru

Затейщикова Елизавета Леонидовна,
студент, Донецкий национальный университет,
г. Донецк, Донецкая Народная Республика
zateyshchikova.liza@mail.ru

Киберпреступность как новая угроза информационному обществу

Данная статья посвящена исследованию киберпреступности как активно развивающемуся явлению, представляющему угрозу современному обществу, где большинство операций с личными данными, банковскими платежами происходят в открытой сети Интернет. По итогам проведенного анализа формулируются выводы, направленные на совершенствование конкретных мер противодействия данному явлению. Предлагается создание Центра по борьбе с киберпреступностью, который будет действовать на уровне Содружества Независимых Государств и заниматься обеспечением эффективного взаимодействия между странами в целях оперативного и результативного противодействия киберпреступности.

Ключевые слова: *киберпреступность, ботнет, компьютерная преступность, кибератаки.*

Karpenko Lyudmila Konstantinovna,
candidate of law, associate professor,
Donetsk national University,
Donetsk, Donetsk people's Republic

Zateyschikova Elizaveta Leonidovna,
student, Donetsk national University,
Donetsk, Donetsk people's Republic

Cyber crime as a new threat to the information society

This article is devoted to the study of cybercrime as an actively developing phenomenon that poses a threat to modern society, where most

transactions with personal data and Bank payments take place on the open Internet. Based on the results of the analysis, conclusions are formulated aimed at improving specific measures to counter this phenomenon. It is proposed to create a center for combating cybercrime, which will operate at the level of the Commonwealth of Independent States and ensure effective interaction between countries in order to quickly and effectively counter cyber crime.

Keywords: *cybercrime, botnet, computer crime, cyber attacks.*

В последние десятилетие в мире набирает обороты такая негативная тенденция, как активный рост числа киберпреступлений. Каждый из нас начинает заботиться о безопасности наших учетных записей, личных данных, которые находятся в сети Интернет.

Подтверждением актуальности исследования киберпреступности в уголовном законодательстве, криминологии, определения способов и средств противодействия ей, является проведение в 2018 году международной компанией Group-IB, которая специализируется на предотвращении кибератак, глобальной международной конференции CyberCrimeCon 2018. Результаты работы конференции представлены новой концепцией информационной безопасности, которая содержится в отчете. В последнем обращено внимание не только на тенденцию к количественному росту киберпреступности, но и на то, что на данный момент только зафиксированными являются 40 активных преступных групп [1].

Рассматривая дефиницию «киберпреступления», исследователи чаще всего относят к данному понятию преступные деяния, совершенные в информационно-телекоммуникационной сфере, либо с ее помощью, либо против нее [2, с. 200].

Необходимо отметить, что данный термин часто употребляется как синоним с термином «компьютерные преступления». В частности, в Российской Федерации предпочтение отдается понятию «компьютерные преступления». Это обусловлено тем, что в Уголовном кодексе Российской Федерации единственной главой, которая предусматривает ответственность за подобные преступления, является Глава 28 «Преступления в сфере компьютерной информации» [7].

В 2001 году было заключено Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации [4]. В ст. 1 Соглашения указывается, что преступления в сфере компьютерной информации – уголовно наказуемые деяния, предметом посягательства которых является компьютерная информация. Отметим, что объектом киберпреступлений выступают отношения информационной безопасности, то есть отношения связанные с созданием, использованием и распространением компьютерной информации.

Из вышеизложенного следует, что рассматриваемые нами термины «киберпреступления» и «компьютерные преступления» действительно очень близки, но все-таки не синонимичны и не тождественны. На наш взгляд, понятие «киберпреступления» является понятием более широким, нежели «компьютерные преступления», поскольку понятие «киберпреступления» более точно отражает природу такого явления, то есть определяется как преступность в информационном пространстве.

В упомянутой 28 Главе Уголовного кодекса Российской Федерации угроза для компьютерной информации рассматривается с точки зрения не совокупности свойств информации, которые нарушаются, а самих действий или бездействий. Следовательно, можно сделать вывод о том, что исследуемая глава не содержит исчерпывающего перечня действий, направленных на посягательство на правоотношения в сфере компьютерной информации. В свою очередь, это также обусловлено беспрерывным развитием компьютерных технологий. Таким образом, даже этот факт уже усложняет расследование преступлений данной категории.

В Модельном Уголовном кодексе государств-участников СНГ также содержится глава о преступлениях в сфере компьютерной информации. Его нормы демонстрируют более широкий подход, предусмотрев ответственность за ряд общественно опасных деяний в Разделе XII «Преступления против информационной безопасности», а именно:

1. Несанкционированный доступ к компьютерной информации;
2. Модификация компьютерной информации;
3. Компьютерный саботаж;
4. Неправомерное завладение компьютерной информацией;
5. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;
6. Разработка, использование и распространение вредоносных программ;
7. Нарушение правил эксплуатации компьютерной системы или сети [3].

Вышеперечисленные позиции Модельного Уголовного кодекса позволяют более тонко дифференцировать уголовную ответственность за преступления в сфере компьютерной информации.

При совершении современных киберпреступлений, как правило, используются модифицированные технологичные средства двух типов: социальную инженерию и вирусную программу.

Первый тип характеризуется телефонной или компьютерной атакой на человека, целью которой является получение личной информации. Пользуясь особенностями психологии личности, киберпреступники могут выдавать себя за другое лицо, вводя человека в заблуждение. Данный метод представляет собой обезличенный контакт с жертвой в сети Интернет и дает большую свободу кибермошенникам.

Второй тип характеризуется тем, что позволяет киберпреступникам удаленно управлять компьютерами без ведома их пользователей с помощью применения «продвинутого» современного программного обеспечения. В этом случае мошенников называют ботами, а сеть – ботнетами.

Ботнет представляется собой совокупность компьютеров, на которых запущено программное обеспечение, позволяющее осуществлять общение между этими компьютерами, а также централизованное или децентрализованное общение с другими компьютерами, предоставляющими команды. Вся эта совокупность компьютеров является зараженной вредоносными программными средствами, и чаще всего, пользователи данных компьютеров не осознают, что они загрузили или были заражены таким программным обеспечением.

Ботнет может использоваться для хищения учетной информации и данных, мошенничества, анонимной массовой рассылки нежелательных сообщений и распространения дополнительных вредоносных программных средств и т. д.

Однозначной трактовки понятия субъектов киберпреступлений в уголовно-правовой науке пока не существуют. Некоторые исследователи считают, что, так как преступления связаны с использованием сложной вычислительной техники, киберпреступления совершаются специальными субъектами. Другие полагают, что имеет место общий субъект, поскольку в современном обществе повышается уровень его компьютеризации [5].

Рассматривая цели совершения киберпреступлений как представления о желаемом результате, необходимо отметить, что здесь наблюдается их разнообразие. Например, экономические цели могут проявляться в виде завладения денежных средств и конфиденциальной информации. Также имеют место быть политические цели, то есть целью совершения преступления является причинение ущерба основным государственным и политическим институтам, подрывающее систему властных отношений и доверия к власти. Существуют и социально-психологические цели – оказание морального, психологического воздействия на граждан. Самой прогрессирующей целью является идеологическая, то есть вербовка интернет-пользователей в ряды различных противозаконных группировок террористического или экстремистского характера.

Пострадавшими от киберпреступлений могут быть и физические, и юридические лица. Таким образом, киберпреступления могут осуществляться в отношении общественных организаций, государственных институтов, иных юридических лиц, а также граждан, то есть их личной информации, свобод или персональной кибербезопасности [6].

По итогам проведенного анализа можно сделать следующие выводы:

1. За последнее десятилетие наблюдается количественный рост совершения киберпреступлений, а также расширение числа преступных группировок, которые используют передовые технологии.

2. Пострадавшими от киберпреступлений являются, как и частные лица, так и организации различного уровня.

3. В условиях всеобщей глобализации нельзя рассчитывать на успех в противоборстве киберпреступности, если это будет в рамках одной страны, то есть необходимо создать устойчивую и эффективную систему межгосударственного сотрудничества.

4. Именно развитие информационных технологий могут дать правоохранительным органам больше возможностей для того, чтобы эффективно координировать совместную деятельность в национальном и международном масштабе.

С учетом вышеизложенного полагаем целесообразным дальнейшее развитие и доработку Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации в целях совершенствования системы и концепции эффективной работы национальных правоохранительных структур, межгосударственной координации и взаимодействия.

Также считаем необходимым создание Центра по борьбе с киберпреступностью, который будет действовать на уровне Содружества Независимых Государств. Данный центр в своей деятельности должен руководствоваться международным законодательством, принципом экстерриториальности и подчиняться напрямую Совету министров внутренних дел государств – участников Содружества Независимых Государств.

Библиографический список

1. Group-IB представила отчет о киберпреступности и призвала рынок к хантингу : офиц. сайт. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 01.12.2019).

2. Словарь международного права / Т. Г. Авдеева, В. В. Алешин, Б. М. Ашавский и др. ; отв. ред. С. А. Егоров. 3-е изд., перераб. и доп. М. : Статут, 2014. 495 с.

3. Модельный Уголовный кодекс (принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств (постановление №7-5 от 17 февраля 1996) (с изм. на 16 ноября 2006) // Электр. фонд правовой и НТД. URL: http://docs.cntd.ru/document/901781490 (дата обращения: 01.12.2019).

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (ратифицировано Федеральным законом РФ от 1 октября 2008 года № 164-ФЗ) // Электр. фонд правовой и НТД. URL: http://docs.cntd.ru/document/902140948 (дата обращения: 01.12.2019).

5. Субъекты преступлений в сфере компьютерной информации // Офиц. сайт группы «Игры разума». URL: http://www.iqpravo.ru/postulati/

kompeternoie-prestuplenij/news_detail. php?I D=1857 (дата обращения: 01.12.2019).

6. Терентьева И. А., Ледяева П. Киберпреступность как современная криминальная угроза // RUSNAUKA. URL: http://www.rusnauka.com/39_ FPN_2016/Pravo/ 5_217686.doc.htm (дата обращения: 01.12.2019).

7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

УДК 343.8

Конардов Сергей Борисович,
старший преподаватель, Костромской государственный университет,
г. Кострома, Российская Федерация
skonardov@ya.ru

Лисенко Наталия Александровна,
магистрант, Костромской государственный университет,
г. Кострома, Российская Федерация
nata.lisenko.97@list.ru

Генезис законодательного регулирования организации исполнения уголовных наказаний, не связанных с лишением свободы, в отношении несовершеннолетних

Статья посвящена изучению и анализу истории досоветского, советского и постсоветского законодательного регулирования назначения и реализации уголовных наказаний, не связанных с лишением свободы, в отношении несовершеннолетних в России. Прослеживается история законодательного закрепления возраста привлечения к уголовной ответственности, а так же зарождение применения к несовершеннолетним осужденным мер воспитательного воздействия.

Ключевые слова: *несовершеннолетний, преступность несовершеннолетних, досоветский период, советский период, постсоветский период, уголовные наказания, не связанные с лишением свободы.*

Konardov Sergey Borisovich,
senior lecturer, Kostroma state University,
Kostroma, Russian Federation

Lisenko Nataliya Aleksandrovna,
postgraduate, Kostroma state University,
Kostroma, Russian Federation