УДК 34 **DOI: 10.34670/AR.2020.78.78.084**

Особенности раннего становления групповых преступлений в киберпространстве

Алексеев Сергей Владимирович

кандидат юридических наук, доцент,
доцент кафедры гражданского и арбитражного процесса.
Самарский государственный экономический университет,
443090, Российская Федерация, Самара, ул. Советской Армии, 141;
e-mail: volga169@yandex.ru

Аннотация

В данной статье рассматриваются особенности зарождения групповых преступлений, совершаемых в киберпространстве. Характеризуются схожие черты как киберпреступлений, так и личностей киберпреступников. Представлены исторические этапы развития киберпреступлений. Помимо этого, в статье анализируются существующие методы противодействия таким преступлениям. Предложены пути, направленные на повышение эффективности по выявлению и противодействию киберпреступности. В работе показано, что в снижении и предотвращении случаев экономической киберпреступности наибольшую отдачу могут дать технологический и организационный подходы. Первый подход предусматривает предотвращение преступлений главным образом за счёт мероприятий технического характера. Организационный подход связан с осуществлением разнообразных организационных мероприятий. Представляется, что российскому законодателю необходимо срочно принимать законы, запрещающие бесконтрольно и обезличенно переводить электронные денежные средства. Как один из выходов в складывающейся ситуации с групповыми преступлениями в киберпространстве видится в том, чтобы окончательно, на законодательном уровне внедрить деанонимизацию любых транзакций. Предложенный выход позволит не только отследить движение денежных средств, но и существенно упростит выявление и установление киберпреступников, их связей.

Для цитирования в научных исследованиях

Алексеев С.В. Особенности раннего становления групповых преступлений в киберпространстве // Вопросы российского и международного права. 2020. Том 10. № 10А. С. 183-191. DOI: 10.34670/AR.2020.78.78.084

Ключевые слова

Преступление, киберпреступность, киберпространство, киберпреступники, хакер, атаки, Интернет, IT-технологии, информационное пространство.

Введение

Информатизация общества — это одна из закономерностей нынешнего остросоциального прогресса. XXI в. - век стремительного развития технологий, которые не перестают трансформироваться, проникая во все сферы общества. В настоящее время трудно представить жизнь без них, именно поэтому инновационные технологические процессы стали неотъемлемой частью жизни всего социума. Трудно сказать, пошло это на пользу или же, наоборот, принесло вред людям. С одной стороны, благодаря инновационной технике появляются аппараты, которые помогают спасти жизнь людям, кроме этого, техника позволяет работать удаленно из любой точки мира. Но, с другой стороны, есть огромные минусы. Один из них - появление киберпреступности, особого вида преступной деятельности, которая совершается с использованием компьютеров через Интернет.

Основная часть

История развития киберпреступности состоит из двух периодов: до и после появления информационной сети «Интернет».

Первый период приходится на 1960-1991 гг. В начале 60-х годов в США компьютеры стоили очень дорого, поэтому были доступны лишь некоторому слою населения, а именно только некоторым государственным органам. В эти годы «компьютерных преступлений» практически не насчитывалось. Они могли состоять лишь в незаконном вмешательстве в компьютерную информацию и персональных данных, их удаление. Ни о каком экономическом вреде пока не говорилось ни слова.

В 70-80-е годы с появления первых персональных компьютеров и прародителя сети «Интернет» – «Арпанет» поспособствовало появлению новых видов киберпреступности.

В 1975 году Агентство передовых исследований Министерства обороны США совместно со Стенфордским и Калифорнийским университетами выпустили первую информационно-телекоммуникационную сеть «Арпанет». Именно в этот период начались многочисленные кибератаки. И только через 2 года был одобрен первый законопроект «О защите федеральных компьютерных систем», в настоящее время он представляет собой § 1030, который включён в Титул 18 Свода законов США.

В СССР первые локальные компьютерные сети появились в конце 1970-х – начале 1980-х гг., а первое экономическое преступление с использованием компьютера в СССР произошло в 1979 году в Вильнюсе, а именно это было хищение 78 584 рублей.

Вначале 1980-х в США появилась информационно-телекоммуникационная сеть «Милнет», которая использовалась только Министерством обороны США. Через несколько лет «Арпанет» и часть «Милнет» соединили и обозначили как «Интернет». Тогда это была совсем небольшая сеть. В эти годы появились такие сети, как «NSFNet» и «USEnet». Количество пользователей в данных сетях ежегодно увеличивалось, что посодействовало увеличению занятием «хакерства». Причем это стало достаточно популярное в обществе увлечение. Складывались все технические условия для появления экономической киберпреступности.

Второй период приходится на 1991 г. и по настоящее время. В 1991 году «Интернет» становится уже мировой информационной сетью, что дало возможность хакерам с любой точки мира совершать преступления. В 1990 году на базе Института атомной энергии им. И. В. Курчатова была разработана Russian Electronic Communication Network, в то же время

появляется доменное имя «.su».

1995 год считается пиком групповых кибер преступлений, поскольку появился первый Интернет-магазин «Amazon»и первый виртуальный банк «Security First Network Bank». Уже в 1997 году в России было зарегистрировано 33 факта совершения компьютерных преступлений. А в 1998 году доступ к сети «Интернет» появился у одного миллиона россиян, что спровоцировало дальнейший рост киберпреступности. В 1998 году было зарегистрировано уже 64 факта совершения компьютерных преступлений, с каждым годом количество таких преступлений увеличивалось, а остановить этот рост было практически невозможно [Простосердов, 2016].

Киберпространство, как виртуальная реальность, существует только на платформе информационно-телекоммуникационной сети. Общим признаком любого киберпреступления является способ его правонарушения-киберпространство. К сожалению, технические нововведения используются не только законопослушными гражданами, но и преступниками. Количество таких преступлений ежегодно только растёт. Достаточно проанализировать официальную статистику МВД России, за январь – ноябрь 2018 г. с использованием компьютерных и информационно-телекоммуникационных технологий было совершено 156 307 преступлений, а за аналогичный период предыдущего года – 824401. По данным Генеральной прокуратуры Российской Федерации, в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65949 до 90587. Проанализировав данные, можно сделать вывод: киберпреступления в Интернете составляют около 4% от числа всех зарегистрированных преступлений в России (это каждое двадцатое преступление). Малоутешительные цифры, к тому же в России весьма низкая раскрываемость экономических киберпреступлений.

Проблемы киберпреступности с каждым днём становятся острее и острее, они не перестают быть актуальными. Это именно те преступления, которые требует незамедлительного вмешательства со стороны правоохранительных органов и государства. Недавно Президент РФ выдвинул ряд мер, направленных на борьбу с экономическими киберпреступлениями:

- создание системы обмена информацией о кибератаках;
- международное сотрудничество;
- использование отечественного программного обеспечения.

Одним из примеров громкого экономического киберпреступления стал всем известный вирус «Petya». Весной 2017 г. по всему миру были зафиксированы атаки вируса-вымогателя «Petya». Этот вирус блокировал операционную систему с предложением последующего выкупа в размере 300 долларов США в биткоинах. Из-за «Petya» пострадали не только пользователи, но и крупные компании, такие, как Сбербанк и Роснефть. Киберпреступники могут действовать как отдельно (преступники-одиночки), так и сообща (кибербанды). По мнению экспертов, чаще всего совершаются групповые хакерские правонарушения. Организованные группы хакеров имеют сложную иерархию, аналогичную мафиозной. Такие банды несут повышенную общественную опасность по сравнению с единоличным преступлением. Для того чтобы разработать эффективные методы борьбы с киберпреступниками, необходимо понимать характеристику их личности.

Криминалисты В.Б. Вехов, Т.М. Лопатина и А.Э. Побегайло делят киберпреступников на следующие основные группы [Побегайло, 2013]:

1. «обычные», которые переносят различные отдельные виды преступной деятельности (мошенничество) в особую среду, предоставляющую уникальные возможности повышения их

«эффективности»;

2. «психически больные». Личность, имеющая психические заболевания, такие как информационная болезнь или компьютерная фобия;

3. киберпреступники, имеющие навыки в информационных технологиях, с помощью которых совершаются преступления, возможные только в киберпространстве (нарушение функционирования сетевых объектов).

Киберпреступления делятся на виды в зависимости от объекта, от предмета посягательства, в зависимости от способов совершения. По объекту посягательства выделяются следующие группы киберпреступлений:

-экономические компьютерные преступления,

-компьютерные преступления против личных прав и неприкосновенности частной сферы,

-компьютерные преступления против общественных и государственных интересов.

Интересен и анализ возрастного состава экономических преступных групп. Этот анализ провели зарубежные исследователи, они отметили, что 43 процента членов преступных кибергруппировок имеют возраст старше 35 лет и лишь 29 процентов - моложе 25 лет [Regoli, Hewitt. DeLisi, 2019]. Цифры значительны, ведь это уже далеко не подростки, совершающие деяния ради развлечений, это уже зрелые люди, с осознанным мировоззрением, которые совершают киберпреступления.

Киберпреступления рассматривают как уголовно караемые действия, предполагающие незаконное попадание в службу компьютерных систем, с задачей модифицирования компьютерных данных. В таком процессе предметом преступления является сам компьютер, а объектом- информационная безопасность. Практически все подобные преступления преследуют экономическую цель, в связи с чем, могут нанести настоящую угрозу не только чьей-либо собственности, но и всей предпринимательской или другой экономической деятельности. Теневое предпринимательство включает в себя почти всю сферу общеэкономических отношений. Нельзя не отметить, ежемесячно растет размер ущерба, который причиняется киберпреступлениями. На просторах Интернета ежедневно появляются новые вакансии с предложениями заняться теневым бизнесом, обещая доход от 15000 тыс. руб. в день. По некоторым расчетам специалистов стало известно, что доходы подобного бизнеса значительно превышают прибыль от незаконной торговли оружиями или специальными веществами. Незаконное предпринимательство - преступление в сфере экономике. Не составит труда сделать вывод, что теневая экономика несет в себе исключительно негативные начала.

Практически все экономические киберпреступления можно разделить на две группы в зависимости от метода их деяния:

1- финансовые киберпреступления, производимые с помощью тонкопсихологического влияния на людей с применением информационной техники (например, хитрость или шантаж);

2-финансовые киберпреступления, производимые с помощью суггестивности на оборудование (например, компьютер или телефон).

Несомненно, развитие информационно - компьютерных технологий способствует развитию активной деятельности преступников. Проблема состоит не только в увеличении числа киберпреступлений, но и в повсеместном распространении таких преступлений во всех сферах. Нередко IT-технологии используют в целях реализации оборота наркотических веществ.

Мотивы к совершению групповых экономических преступлений в киберпространстве:

1) Корыстный характер;

2) Высокий уровень латентности;

3) Довольно значительно расстояние между преступником и «жертвой»;

4) Множественный характер;

5) Сложность определения персональной ответственности;

6) Анонимность и коллективность жертв.

Чаще всего кибербанда совершает преступления против собственности. Наиболее популярными являются следующие:

a. Мошенничество в сфере кредитования (ст.159.1 УК РФ);

b. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

c. Вымогательство (ст. 163 УК РФ);

d. Причинение имущественного ущерба путём обмана и злоупотребления доверием (ст. 165 УК РФ);

e. Умышленное уничтожение или повреждение чужого имущества (ст. 167 УК РФ).

Сложная эпидемиологическая и экономическая ситуация, вызванные COVID-19 в 2020 г. сопровождаются ростом активности кибермошенников. Апрель и май 2020 г. стали рекордными по числу успешных кибератак. Причем популярностью у преступников пользовались востребованные во время пандемии товары - маски, перчатки, санитайзеры. Один банк фиксировал в среднем 400-600 таких мошеннических попыток в месяц, средний размер одного перевода - более 7 тысяч рублей. Согласно данным МВД России число преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на 94,6 процента.

Основная цель – извлечение прибыли, при нежелании платить налоги государству. Иногда подобный бизнес нацелен также на причинение крупного ущерба гражданам или предприятиям. Реализация такой экономической деятельности при неимении лицензии образует состав преступления, предусмотренного ст. 171 УК РФ «Незаконное предпринимательство».

Видов предпринимательской деятельности в киберпространстве много. Наиболее популярными являются следующие:

– Электроннаякоммерция;

– Банковскаядеятельность;

– Рекламнаядеятельность;

– Оказание различных услуг (например, оформление сайтов).

Легализация денежных средств или другого какого-либо имущества, приобретённого преступным путём, является преступлением международного уровня. Для противодействия было принято множество международных соглашений и конвенций, такие как Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности, Конвенция ООН против транснациональной организованной преступности и многие другие.

Способы легализации денег в киберпространстве можно условно разделить на следующие группы:

- легализация денежных средств с использованием существующих сайтов (социальные сети);

- легализация денежных средств с помощью открытия новых сайтов (Интернет-магазин);

- легализация денежных средств с использованием Интернет-банкинга;

- легализация денежных средств с использованием криптовалют.

Интернет-магазиныи, Интернет-казино, как правило, используются для отмывания денежных средств, полученных преступным путём в особо крупном размере. Стоит отметить,

что для поддержания нормального функционирования таких сайтов нужен постоянный контроль за оборудованием и финансовыми операциями.

Для перевода денег в киберпространстве Интернет-банками создаются специальные системы обслуживания: пластиковые карты или предоставление доступа к счетам напрямую через «Интернет», выпуск собственных Интернет-валют. Множество банков не контролируют поток такой Интернет-валюты и даже не взимают комиссию за перевод, что создаёт условия для легализации «грязных» денежных средств с помощью данной системы. К примеру, в России данная система используется в картах «QIWI Wallet» от «Visa», для приобретения которых требуются только номер телефона, никаких паспортных данных предоставлять не нужно. Эти особенности делают держателей данных карт анонимными и создают все условия для отмывания денег.

Один из самых легких и доступных для всех способов экономической киберпреступности является продажа несуществующего имущества или товара через сайты-объявления, например Avito.ru, Юла. Преступник регистрируется на сайте, выставляя какое-либо объявление о несуществующем товаре. Например, продажа редких, драгоценных монет. Находит покупателей в другом городе, предлагает товар и просит перевести предоплату. Когда покупатель переводит предоплату, преступник попросту удаляет свой аккаунт. Причём деньги просит перевести через терминалы оплаты, такие как Яндекс. деньги, Киви и другие. На сегодняшний момент такие противоправные деяния совершаются ежедневно не один раз.

Схожая ситуация на сайтах-аукционах. Преступник создаёт множество ложных аккаунтов на сайте Интернет-аукциона. С одного выставляет предмет на аукцион, а с остальных создаёт ложный спрос, искусственно повышая цену. Виновный в одном лице является как продавцом, так и покупателем.

Особенность вышеперечисленных способов заключается в том, что их может осуществить всего один человек, который особо не обладает специальными техническими знаниями, так как он будет использовать существующую инфраструктуру.

К другим киберпреступлениям, нередко совершаемым в сфере экономической деятельности, можно отнести фальсификацию Единого Государственного Реестра юридических лиц, валютные преступления, налоговые преступления, фиктивное банкротство и коммерческий подкуп.

Нарастающая ситуация киберпреступности требует незамедлительного применения мер противодействия им. Поскольку основные цели внутренней политики Российской Федерации — это обеспечение защиты граждан, укрепление обороноспособности страны, повышение уровня правопорядка, в Российской Федерации разработали систему мер противодействия, которая направлена на:

1) обнаружение, предотвращение либо снижение и ослабление факторов экономической киберпреступности;

2) обнаружение и предотвращение ситуаций, напрямую побуждающих на совершение экономических преступлений в киберпространстве;

3) обнаружение лиц повышенного криминального риска и предотвращение этого риска;

4) обнаружение лиц, действия которых указывают на вероятность совершения экономических киберпреступлений, также оказание на них регулирующего воздействия. Вышеперечисленные меры можно разделить на две основные группы: правовые и криминологические. Первые - правовые - направлены на устранение недостатков законодательства. Данные меры включают в себя предложения по усовершенствованию

законодательства: об уголовной ответственности за экономические преступления и преступления в сфере компьютерной информации; законодательства об информации, о персональных данных. Правовые меры гарантируют их исполнение на законодательном уровне. Вторые - криминологические - включают предложения по противодействию таким терминам финансовой киберпреступности, как анонимность злоумышленников, иммунитет преступлений, отсутствие культуры информационной безопасности у населения. Такие меры содержат предложения по профилактике цифровой безопасности среди отдельных групп населения, предложения по модернизации информационных технологий, а также предложения по «мастерству» финансовых преступлений в киберпространстве.

Заключение

Несомненно, правительство ведет борьбу с киберпреступностью и преступлениями, совершаемыми с использованием IT-технологий. Но в современном мире этого пока недостаточно. Такие преступники намного хитрее, они гораздо быстрее осваивают всю платформу Интернета.

На государственном и уровне частных предприятий нужно активно заниматься просветительской деятельностью для повышения компетенции в сфере компьютерных технологий отдельных пользователей, сотрудников компаний, которые смогут уменьшить риск стать жертвой киберпреступлений. Необходимо проводить уроки, лекции по компьютерной грамотности населения, ведь это поможет лучше понимать все угрозы, связанные с работой в социальных сетях.

Помимо вышесказанного, в снижении и предотвращении случаев экономической киберпреступности наибольшую отдачу могут дать технологический и организационный подходы. Первый подход предусматривает предотвращение преступлений главным образом за счёт мероприятий технического характера. Организационный подход связан с осуществлением разнообразных организационных мероприятий. Представляется, что российскому законодателю необходимо срочно принимать законы, запрещающие бесконтрольно и обезличенно переводить электронные денежные средства. Как один из выходов в складывающейся ситуации с групповыми преступлениями в киберпространстве видится в том, чтобы окончательно, на законодательном уровне внедрить деанонимизацию любых транзакций. Предложенный выход позволит не только отследить движение денежных средств, но и существенно упростит выявление и установление киберпреступников, их связей.

Библиография

1. Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: Монография. / Дворецкий М.Ю., Копырюлин А.Н. Тамбов, ТГУ им. Г.Р. Державина. 2006. С.15.
2. Дремлюга Р.И. Интернет-преступность: Монография. Владивосток, Изд. Дальневосточного университета. 2008. С. 42.
3. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005. С.27
4. Киданова Н.Л. Актуальные проблемы современности - экономические преступления, совершаемые в киберпространстве.
5. Побегайло А.Э. Киберпреступность: лекция / А.Э. Побегайло. − М., Академия Генеральной прокуратуры Российской Федерации. 2013. − 50 с
6. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. …канд. юрид. наук. Москва, 2016. С.17

7. «Federal Criminal Code and Rules» / Title 18 – Crime and Criminal Procedure - § 1030 Fraud and related activity in connection with computers - (amendment received to February 15, 1999), West Group, St. Paul, Minn, 1999. – p. 632 – 634.
8. Johnson T. Hate Crimes in Cyberspace //Syracuse J. Sci. & Tech. L. – 2017. – T. 34. – C. 16.
9. Kadir N. K., Judhariksawan J., Maskun M. Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes //FIAT JUSTISIA: Jurnal Ilmu Hukum. – 2019. – T. 13. – №. 4. – C. 333-344.
10. Pawlak P. A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace //EU Institute for Security Studies, July. – 2017.

Features of early formation of group crimes in cyberspace

Sergei V. Alekseev

PhD in Law, Associate Professor,
Associate Professor of the Department of Civil and Arbitration Process.
Samara State University of Economics,
443090, 141 Sovetskoi Armii st., Samara, Russian Federation;
e-mail: volga169@yandex.ru

Abstract

This article examines the peculiarities of the origin of group crimes committed in cyberspace. Similar features of both cybercrimes and cybercriminals ' personalities are characterized. The historical stages of cybercrime development are presented. In addition, the article analyzes the existing methods of countering such crimes. The ways aimed at improving the effectiveness of detecting and countering cybercrime are proposed. The paper shows that technological and organizational approaches can give the greatest impact in reducing and preventing cases of economic cybercrime. The first approach involves the prevention of crimes mainly through technical measures. The organizational approach is associated with the implementation of a variety of organizational activities. It seems that the Russian legislator urgently needs to pass laws prohibiting uncontrolled and impersonal transfer of electronic funds. As one of the ways out in the current situation with group crimes in cyberspace, it is seen in finally introducing deanonymization of any transactions at the legislative level. The proposed solution will not only track the flow of funds, but also significantly simplify the identification and establishment of cybercriminals and their connections.

For citation

Alekseev S.V. (2020) Osobennosti rannego stanovleniya gruppovykh prestuplenii v kiberprostranstve [Features of early formation of group crimes in cyberspace]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 10 (10A), pp. 183-191. DOI: 10.34670/AR.2020.78.78.084

Keywords

Crime, cybercrime, cyberspace, cybercriminals, hacker, attacks, internet, IT technologies, information space.

References

1. Dvoretsky M. Yu., Kopyryulin A. N. Optimization of criminal responsibility and problems of qualification of crimes in the sphere of computer information: Monograph. / Butler, M. Yu., Kaparulin A. N. Tambov, TGU named. G. R. Derzhavin. 2006. P. 15.
2. Dremlyuga R. I. Internet crime: Monograph. Vladivostok, Far Eastern University Publishing House. 2008. P. 42.
3. Tropina T. L. Cybercrime: concept, state, criminal - legal measures of struggle: dis. ... cand. the faculty of law. sciences'. Vladivostok, 2005. P. 27
4. Kidanova N. L. Actual problems of our time - economic crimes committed in cyberspace.
5. Pobegailo A. E. Cybercrime: a lecture / A. E. Pobegailo. - M., Academy of the General Prosecutor's Office of the Russian Federation. 2013. − 50 s
6. Prostoserdov M. A. Economic crimes committed in cyberspace and measures to counteract them: dis. ... cand. the faculty of law. sciences'. Moscow, 2016. P. 17
7. "Federal Criminal Code and Regulations" / Title 18-Crimes and Criminal Procedure - § 1030 Fraud and Related activities in connection with Computers - (Amendment received February 15, 1999), Western Group, St. Paul, Minnesota, 1999. - p. 632-634.
8. Johnson, T. (2017). Hate Crimes in Cyberspace. *Syracuse J. Sci. & Tech. L.*, *34*, 16.
9. Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes. *FIAT JUSTISIA: Jurnal Ilmu Hukum*, *13*(4), 333-344.
10. Pawlak, P. (2017). A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace. *EU Institute for Security Studies, July*.