Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2023. – Т. 9 (75). № 2. – С. 306–312.

УДК 343.231

ЛИЧНОСТЬ ИНТЕРНЕТ-ПРЕСТУПНИКА И ОТДЕЛЬНЫЕ СПОСОБЫ ИХ ВЫЯВЛЕНИЯ В ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ

Зоз В. А., Лагуточкина А. С.

В статье раскрывается вопрос определения понятия киберпреступления, дается характеристика личности интернет-преступника, рассмотрены некоторые способы выявления данной категории преступников в глобальной сети. В частности, Европейской комиссией предложено интерпретировать понятие киберпреступности как: «традиционная форма преступления, совершенного с помощью электронных коммуникационных сетей и информационных систем, а также публикация информации, нарушающей права третьих лиц, через электронные медиа источники, преступления, присущие только электронным сетям». Определено что относится к основным свойствам киберпреступности, а именно: интеллектуальный характер киберпреступности, отсутствие возрастного ценза и социального статуса, анонимность и неперсонифицированность, дистанцированность киберпреступлений, транснациональность киберпреступлений. Проведена классификация киберпреступлений по категориям. При изучении личности интерне-преступника установлено, что данная категория лиц владеет навыкам использования компьютерной техники и других электронных средств, как правило, либо это любители, то есть те, которые действуют самостоятельно, в домашних условиях и свободное от работы время, либо высокообразованные специалисты, которые действуют в составе организованных преступных групп.

Известны типы сетевых объектов, содержащие информацию о киберпреступлениях: сетевые объекты, на которых повторяются попытки преступных посягательств и существуют условия для их осуществления; сайты, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту; места сетевого общения криминально настроенных лиц. В связи с чем борьба с преступлениями в рассматриваемой сфере осуществляется в двух основных направлениях: выявление лиц, которые готовят совершение преступления и выявление лиц, виновных в совершении преступления, то есть уже после факта совершения преступления.

Ключевые слова: киберпреступления, личность интернет-преступника, оперативные подразделения органов внутренних дел, Интернет, социальная сеть, сетевые объекты.

Стремительное развитие и повседневное применение информационных технологий, преобразование информации в важнейший ресурс жизнедеятельности, обуславливает движение человечества к информационному обществу. Информационная революция привнесла в нашу жизнь новые действенные возможности, открыла невиданные перспективы: упростила доступ к информации, дала возможность обрабатывать большие массивы информации и пр.

Однако, по мере появления различных достижений науки и техники большинство из них берутся на вооружение и преступным миром. Совершенствование компьютерной техники, внедрение ее во всех сферах человеческой деятельности сыграло наиболее существенную роль в техническом вооружении преступности. Ориентирование криминальных структур на использование высоких информационных технологий объясняется доступностью и рентабельностью последних.

Под киберпреступностью (также компьютерными преступлениями) понимают использование информационных технологий как инструмента для совершения незаконных действий, таких как мошенничество, детская порнография, нарушение права интеллектуальной собственности и персональных данных и пр.

На заседании Генеральной Ассамблеи ООН, где обсуждался вопрос киберпреступности, одним из пунктов обсуждения было определение данного понятия. Так, его трактовка главным образом зависит от того, в каком контексте будет использо-

ваться этот термин. Основу киберпреступности составляет довольно ограниченный круг деяний, направленных на нарушение конфиденциальности, целостности и доступности компьютерных данных или систем [9].

Европейская комиссия в 2007 г. предложила такую интерпретацию понятия киберпреступности: «традиционная форма преступления, совершенного с помощью электронных коммуникационных сетей и информационных систем, а также публикация информации, нарушающей права третьих лиц, через электронные медиа источники, преступления, присущие только электронным сетям» [10].

Несмотря на принятые международные и национальные законодательные по борьбе с киберпреступностью в ряде стран, в том числе и в России, ее «унифицированный» состав до сих пор четко не определен, поскольку как возможности технических средств, программного обеспечения, средств телекоммуникации, так и уголовные ухищрения самих киберпреступников, непрерывно растут с развитием научно-технического прогресса. За последние несколько лет было сформулировано понятие «киберпреступности», под которой понимают преступность в традиционном смысле этого слова, но которая совершается в сети Интернет [6].

К основным свойствам киберпреступности необходимо отнести следующие: интеллектуальный характер киберпреступности; отсутствие возрастного ценза и социального статуса; анонимность и неперсонифицированность; дистанцированность киберпреступлений; транснациональность киберпреступлений.

В целом специфика преступности в сети Интернет заключается в следующем: относительной комфортности, то есть приготовление и совершение преступления осуществляется практически не отходя от «рабочего места»; доступности – в связи с тенденцией постоянного снижения цен на компьютерную технику; широкой географии совершения преступлений, но учитывая то, что основное количество компьютеров расположено в крупных населенных пунктах, то есть именно на них и приходится «львиная доля» преступности; удаленности объекта преступных посягательств – он может находиться за тысячи километров от места совершения преступления; сложности обнаружения, фиксации и изъятия криминалистически значимой информации (следовой картины преступления) при выполнении следственных действий для использования ее в качестве вещественного доказательства и т.д.; широком использовании преступниками средств шифрования информации [4].

Киберпреступления можно разделить на три категории: исключительно сетевые преступления, где цифровые системы являются основной целью, но одновременно выступают и средствами посягательства. Эта категория включает в себя посягательство на компьютерные системы для уничтожения инфраструктуры интернет-технологий и незаконное завладение данными; обычные преступления, которые были переведены в плоскость киберпреступлений в связи с использованием Интернета; использование Интернета с целью торговли наркотиками и как вспомогательный инструмент для других видов преступлений.

Однако необходимо различать преступления, совершенные через Интернет, и такие же, но осуществленные оффлайн. Например, переписка о возможном плане преступления не будет считаться киберпреступлением, поскольку в нем отсутствует состав преступления, можно лишь предположить ход событий, а уже его непосредственная реализация находится за пределами Интернета.

Личность преступника, совершающего преступления в сети Интернет является одним из основных элементов оперативно-розыскной характеристики. Пол, возраст, образование, место жительства, наличие судимости – это сведения, необходимые для составления характеристики личности преступника, совершающего такие неправомерные действия. Так, на вопрос, способно ли повысить эффективность по выявлению и раскрытию преступлений в сети Интернет знание оперативными сотрудниками особенностей лиц, совершающих данные преступления, 96 % опрошенных сотрудников ответили утвердительно. Лишь 4 % затруднились с ответом. Отсюда следует, что практические работники осознают необходимость изучения личностных особенностей Интернет-преступников для успешной борьбы с преступлениями данной категории.

В литературе высказываются различные точки зрения относительно определения сущности такого элемента преступления как личность преступника. Одни ученые определяют личность преступника как социально-биологическую систему, свойства и признаки которой отражаются в материальной среде и используют для раскрытия и расследования преступлений (к таким свойствам относятся: физические, биологические и социальные).

По мнению других, личность преступника – это понятие, выражающее сущность лица, совершившего преступление, а к системе признаков личности преступника относят данные демографического характера, некоторые моральные свойства и психологические особенности. Третьи же включают в данное понятие совокупность информации о личности преступника, которая составляет его характеристику, все те данные, которые могут определять эффективные пути розыска и изобличения преступника, и связанные с этим задачи расследования [5].

Как видно из приведенных подходов, большинство юристов выделяют следующие элементы характеристики личности преступника: социальные – социальное положение, образование, национальность, семейное положение, профессия и т. п.; психологические – мировоззрение, убеждения, навыки, привычки, эмоции, чувства, темперамент и пр.; физиологические – анатомические и функциональные признаки, биохимические особенности крови, слюны и т. д. [1].

По сравнению с традиционными видами преступности интернет-преступность более «молода». По статистике возраст лиц, совершающих преступления в сети Интернет, достигает от 15 до 45 лет. Проведенное исследование уголовных дел показало, что на момент совершение противоправных действий возраст 33 % преступников не превышал 20 лет, 13 % были старше 40 лет, 54 % имели возраст от 20 до 40 лет. Практика показывает, что все чаще такими преступниками становятся несовершеннолетние.

Интернет-преступниками являются лица, владеющие навыкам использования компьютерной техники и других электронных средств: а) любители, то есть те, которые действуют самостоятельно, в домашних условиях и свободное от работы время, б) высокообразованные специалисты, которые действуют в составе организованных преступных групп.

Криминальная практика свидетельствует, что некоторые преступники данной группы действуют без соучастников, тогда как большинство из них совершают преступления в составе организованных преступных группировок. В такие группы могут входить работники банковских учреждений, различных коммерческих структур,

вычислительных центров банковских учреждений и пр. Следует отметить, что в состав такой группы обязательно входит один или несколько участников, которые являются программистами или хотя бы обладают знаниями и навыками в области компьютерных информационных технологий [3].

В литературе отмечается, что при изучении личности интернет-преступника следует обратить внимание на роль навыков и привычек, свойственных каждому человеку. При расследовании преступлений, совершаемых в Сети, изучение этих качеств имеет большое значение для розыска, выявления преступников, так как нередко именно навыки и привычки лица влияют на избираемый способ и механизм совершения преступления. Среди признаков, имеющих самостоятельное значение при выявлении интернет-преступников называют профессиональные и преступные навыки правонарушителя. Знание привычек и навыков лица играет определенную роль из-за того, что эти качества человека индивидуализируют его противоправное деяние, и чем специфичнее и сложнее навык, тем больше времени и усилий требуется на его освоение, тем выше его оперативно-розыскная значимость [8].

Преступления, совершаемые в Сети, совершенные в составе группы, имеют широкий спектр видовых отличий. Можно выделить преступления, совершенные организованной группой (35 %); совершенные международной организованной группой (9 %); совершенные группой лиц по предварительному сговору (56 %).

Итак, можно выделить те свойства личности интернет-преступника, изучение которых позволяет разработать рекомендации для избрания правильного направления выявления преступников, обеспечения наиболее эффективной тактической линии при производстве розыскных действий; установить, какие черты этого лица должны учитываться при выявлении данного вида преступлений.

Личность интернет-преступника характеризуется специфическим комплексом признаков. Большинство преступников имеют сильный дар воображения, используют влияние и умение убеждать людей. В некоторых случаях одним из важных качеств личности интернет-преступника есть наличие организаторских способностей, т.к. некоторые виды киберпреступлений являются технически сложными в плане исполнения, а потому в их совершении могут участвовать несколько людей [2].

Одним из основных направлений деятельности оперативных подразделений правоохранительных органов в борьбе с преступностью является выявление лиц, готовящихся к совершению преступления или совершающих его.

В научных кругах сложились различные взгляды на содержание данного понятия, и это обусловлено тем, что они рассматривают его с разных позиций. Так В.В. Лысенко считает, что выявить преступление означает установить, зафиксировать, определить факт и обстоятельства совершения общественно опасного деяния [7].

Стоит заметить, что обнаружение лиц, совершающих преступления в Сети, может происходить в процессе оперативного поиска, оперативной разработки. В первом случае речь идет о поиске ответа на вопрос, было преступление или нет, что в большей степени имеет отношение к событию преступления. А во втором обнаружение может происходить в процессе оперативной разработки, как комплекс оперативно-розыскных мероприятий, проведенных в отношении лица или группы лиц, обоснованно подозреваемых в подготовке или совершении преступления и др. [10].

Чаще всего выявление преступлений или лиц причастных к ним начинается с получения первичной информации, содержащей сведения о признаках преступления.

Анализируя данную информацию, сотрудники оперативных подразделений осуществляют познание процессов, происходящих в криминальной среде, устанавливают тенденции их изменения. Для уточнения и проверки сведений, которые проводятся путем сопоставления и сравнения с другими сведениями, необходимо получение дополнительной информации. Это позволяет найти недостающие сведения, несоответствия между рассматриваемыми данными и сделать вывод о наличии или отсутствии признаков подготовки или совершения преступления [11].

Выделим следующие основные типы сетевых объектов, содержащие информацию интересную для оперативных подразделений: а) сетевые объекты, на которых повторяются попытки преступных посягательств и существуют условия для их осуществления; б) сайты, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту; в) места сетевого общения уголовно настроенных лиц.

Важные для выявления незаконных действий сведения концентрируются на сетевых ресурсах в виде следов противоправной деятельности, ссылок на материалы, запрещенные к распространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения противозаконных действий.

Борьба с преступлениями в рассматриваемой сфере осуществляется в двух основных направлениях: выявление лиц, которые готовят совершение преступления; выявление лиц, виновных в совершении преступления, то есть уже после факта совершения преступления. Получение информации в отношении конкретного лица, которое готовит совершение преступления в Сети, является приоритетным направлением в работе правоохранительных органов, что обусловлено возможностью предотвратить совершение преступления и наступление его последствий. Но, как показывает практическая деятельность, реализовать это направление сложно.

Лица, совершающие преступления данного вида, тщательно скрывают свои преступные намерения и действия. Поэтому важны любые, даже случайные, отрывочные, неподтвержденные данные из разных источников, в которые своей совокупности могут достаточно убедительно указывать на возможную причастность лица к совершению преступления. Полученная информация концентрируется в различных информационных системах правоохранительных органов с целью постоянного отслеживания деятельности лиц, совершающих преступления в сети.

Список литературы:

1. Алауханов Е. Криминология: учебник. Алматы, 2008. С. 5.
2. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. … канд. юрид. наук. Московская гос. юрид. акад. им. О.Е. Кутафина. М., 2012. С. 15.
3. Бабакова М.А. Психологические аспекты розыска при расследовании преступлений, совершенных с использованием современных технологий // Вестник криминалистики. М.: Спарк, 2009. № 2 (30). С. 110.
4. Бабакова М.А. Особенности расследования киберпреступлений // Юридическая наука и правоприменение: сб. науч. трудов. Саратов: Изд-во ГОУ ВПО «Саратовская государственная академия права», 2009. С. 192–193.
5. Ермолович В.Ф. Криминалистическая характеристика преступлений. Мн.: Амалфея, 2001. 194 с.
6. Лагуточкин А.В. Некоторые особенности использования информационного пространства сети интернет в борьбе с преступностью // Проблемы законодательного регулирования Интернет-ресурсов и правового разрешения конфликтов с участием субъектов Интернет-сообщества: материалы международной научно-практической конференции в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине». Белгородский государственный национальный исследовательский университет. 2013. С. 125–129.

7. Лысенко В.В. О практике расследования уголовных дел о преступлениях в сфере банковской деятельности. URL: https://cyberleninka.ru/article/n/o-praktike-rassledovaniya-ugolovnyh-del-o-prestupleniyah-v-sfere-bankovskoy-deyatelnosti
8. Чулахов В.Н. Криминалистическое исследование навыков и привычек человека. М., 2004. С. 162.
9. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Вена, 25-28 февраля 2013. С. 21.
10. Home Affairs Committee E-crime Fifth Report of Session 2013–14 // Ordered by the House of Commons. 17 July 2013. P. 115.
11. Иванов С.И. Особенности проведения оперативно-разыскных мероприятий в сети Интернет // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2018. № 18-1. С. 23–24/
12. Зоз В.А., Лагуточкина А.С. Отдельные элементы современного состояния противодействия преступлениям, совершенным с использованием социальных сетей, в отношении несовершеннолетних // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 9. № 4. С. 292–298.

Zoz V.A., Lagutochkina A.S. Individual elements of the current state of countering crimes committed using social networks against minors // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2023. – T. 9 (75). № 2. – P. 306–312.

The article reveals the definition of cybercrime, characterizes the personality of an Internet criminal, considers some ways to identify this category of criminals in the global network. In particular, the European Commission proposed to interpret the concept of cybercrime as: "a traditional form of crime committed by means of electronic communication networks and information systems, as well as the publication of information that violates the rights of third parties, through electronic media sources, crimes inherent only in electronic networks". It was defined that refers to the main features of cybercrime, namely: the intellectual nature of cybercrime, the lack of age qualification and social status, anonymity and non-personalization, distance of cybercrime, transnationality of cybercrime. The classification of cybercrime by category was made. When studying the personality of cybercriminals, it was established that this category of offenders possess skills in the use of computer technology and other electronic means, as a rule, either they are amateurs, that is, those who act independently, at home and in their spare time, or highly educated specialists who act as part of organized criminal groups. It should be noted the following main types of network objects, which contain information on cybercrime: network objects, which repeat attempts of criminal encroachments and there are conditions for their implementation; sites through which socially dangerous information is spread, sold items prohibited for circulation; places of network communication of criminally inclined persons. In this connection, the fight against crimes in the area under consideration is carried out in two main directions: revealing of persons, who prepare committing a crime and revealing of persons, who are guilty of committing a crime, that is, after the fact of committing a crime.

Keywords: cybercrime, personality of the Internet criminal, operative divisions of bodies of internal affairs, Internet, social network, network objects.

Spisok literatury:

1. Alauhanov E. Kriminologiya: uchebnik. Almaty, 2008. S. 5.
2. Atamanov R.S. Osnovy metodiki rassledovaniya moshennichestva v seti Internet: avtoref. dis. … kand. yurid. nauk. Moskovskaya gos. Yurid. Akad. Im. O.E. Kutafina. M., 2012. S. 15.
3. Babakova M.A. Psihologicheskie aspekty rozyska pri rassledovanii prestuplenij, sovershennyh s ispol'zovaniem sovremennyh tekhnologij // Vestnik kriminalistiki. M.: Spark, 2009. № 2 (30). S. 110.
4. Babakova M.A. Osobennosti rassledovaniya kiberprestuplenij // yuridicheskaya nauka i pravoprimenenie: sb. Nauch. Trudov. Saratov: Izd-vo GOU VPO «Saratovskaya gosudarstvennaya akademiya prava», 2009. S. 192–193.
5. Ermolovich V.F. Kriminalisticheskaya harakteristika prestuplenij. Mn.: Amalfeya, 2001. 194 s.
6. Lagutochkin A.V. Nekotorye osobennosti ispol'zovaniya informacionnogo prostranstva seti internet v bor'be s prestupnost'yu // Problemy zakonodatel'nogo regulirovaniya Internet-resursov i pravovogo razresheniya konfliktov s uchastiem sub"ektov Internet-soobshchestva: materialy mezhdunarodnoj nauchno-prakticheskoj konferencii v ramkah proekta «Rossijsko-ukrainskie kriminalisticheskie chteniya na Slobozhanshchine». Belgorodskij gosudarstvennyj nacional'nyj issledovatel'skij universitet. 2013. S. 125–129.
7. Lysenko V.V. O praktike rassledovaniya ugolovnyh del o prestupleniyah v sfere bankovskoj deyatel'nosti. URL: https://cyberleninka.ru/article/n/o-praktike-rassledovaniya-ugolovnyh-del-o-prestupleniyah-v-sfere-bankovskoy-deyatelnosti
8. Chulahov V.N. Kriminalisticheskoe issledovanie navykov i privychek cheloveka. M., 2004. S. 162.
9. Vsestoronnee issledovanie problemy kiberprestupnosti i otvetnyh mer so storony gosudarstv-chlenov, mezhdunarodnogo soobshchestva i chastnogo sektora // Vena, 25-28 fevralya 2013. S. 21.
10. Home Affairs Committee E-crime Fifth Report of Session 2013–14 // Ordered by the House of Commons. 17 July 2013. P. 115.

11. Ivanov S.I. Osobennosti provedeniya operativno-razysknyh meropriyatij v seti Internet // Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami. 2018. № 18-1. S. 23–24.
12. Zoz V.A., Lagutochkina A.S. Otdel'nye elementy sovremennogo sostoyaniya protivodejstviya prestupleniyam, sovershennym s ispol'zovaniem social'nyh setej, v otnoshenii nesovershennoletnih // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Yuridicheskie nauki. 2022. T. 8. № 4. S. 292–298.
.