ТИПОЛОГИЯ ЛИЧНОСТИ КОМПЬЮТЕРНЫХ ПРЕСТУПНИКОВ: КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ

Сергеенкова Виктория Сергеевна

обучающаяся, ФГКОУ ВО Московская академия СК России, РФ, г. Москва

Кравцов Дмитрий Александрович

научный руководитель, канд. юрид. наук, доцент, полковник юстиции, ФГКОУ ВО «Московская академия СК России», РФ, г. Москва

Аннотация. Полномасштабное развитие компьютерных технологий имело одним из своих последствий прогрессирующее увеличения количества совершаемых ежегодно компьютерных преступлений. В настоящей статье на основе теоретических трудов криминологов выделена типология личности и компьютерных преступников и определено ее значение для решения практических задач.

Ключевые слова: киберпреступность, хакер, компьютерные преступления, типология личности, компьютерные технологии, цифровая безопасность.

Компьютерные технологии на сегодняшний день полностью проникли во все сферы жизни общества, и даже работу государственных учреждений и систем невозможно представить без доступа к сети Интернет. Стремительное развитие компьютерных технологий и глобальных информационных и телекоммуникационных сетей предопределило особый интерес к проблеме информационной (цифровой) безопасности, поскольку число киберпреступлений с каждым годом лишь увеличивается. Согласно официальным статистическим данным МВД России, удельный вес таких преступлений за 2021 год составил более четверти от общего массива, причем годовой прирост в 1,4% [1] по сравнению с аналогичным показателем за 2020 год, который представлен 73,4% [2], может в свою очередь свидетельствовать о положительных тенденциях в системе мер предупреждения. Возможной причиной такой динамики мы считаем создание в системе Следственного комитета РФ в конце 2019 года отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий, который был призван концентрировать усилия в борьбе с киберпреступностью [3].

При этом одним из важнейших факторов, обуславливающих высокий уровень общественной опасности киберпреступлений, является то, что они могут стирать границы отдельных государств, и носят транснациональный и трансграничный характер, что создает дополнительные трудности при расследовании данной категории преступлений ввиду необходимости консолидации с правоохранительными органами зарубежных стран, а пока механизм международно-правового взаимодействия реализуется на практике с довольно большими трудностями ввиду, в том числе нестабильной политической обстановки в мире.

Рассматривая особенности личности киберпреступников, нельзя не заметить, что большая часть из них, совершая свои преступления, имеет корыстный мотив, т.е. являются кибермошенниками. Однако также стоит рассмотреть лиц, чья заинтересованность строится на хулиганских побуждениях, а также неосторожных киберпреступников [9, С. 120].

Среди основных типологий личности киберпреступников известна выделенная В.В. Крыловым [5, С. 63-66], которая несмотря на прошедшие годы не потеряла своей актуальности и лишь приобрела новые черты, свойственные современному этапу развития преступности и информационных технологий. Кроме того, свои классификации были предложены В. Повышевым [7, С. 9-11] и А.Л. Осипенко [6, С. 205-223]. На их основе видится возможность выделить следующие типы компьютерных преступников, действующих в современной России:

а) «Неосторожные» киберпреступники совершают свои преступления по причине недостаточной компьютерно-технической осведомлённости. Возможным мотивом у данной категории может выступать желание ознакомиться с какой-либо информацией или получить определенный цифровой продукт бесплатно, однако при этом они не осознают противоправности своих действий;

б) «Кибершпионы», чьей специализацией является хищение сведений о личных, экономических, политических и иных конкурентах «заказчика». Кроме того, целью их деятельности могут быть важные промышленные и технические планы и разработки, в том числе и государственного значения. Особенностью этой группы является их высокий уровень «профессиональной» подготовленности;

в) «Киберхулиганы», которые совершают преступления, как правило, с целью получения удовольствия от процесса преодоления защитных компьютерных систем. Их деятельность носит нерегулярный характер и отличается невысоким уровнем профессионализма [4, С. 59];

г) «Хактивисты», чьим основным мотивом является идеология, которую они стремятся продвигать посредством кибератак в мировой компьютерной сети. Стоит отметить, что сама их идеология имеет протестный характер и строится на недоверии к государственной власти и принципе свободы информации, поэтому чаще всего жертвами хакактивистов становятся государственные структуры и учреждения, крупные коммерческие организации и публичные личности, каким-либо образом противоречившие их идеям;

д) Хакеры, для которых компьютерная преступность является «профессиональной» сферой деятельности. Их отличают глубокие познания в области компьютерных технологий и цифровой безопасности. При этом в криминологии их подразделяют на «белых хакеров» и «черных хакеров». Первые не преследуют преступного умысла, а их действия обусловлены желанием найти уязвимые места в системе компьютерной безопасности с целью их последующего исправления. Для вторых же движущим является именно корыстный мотив, который направляет их на причинение ущерба данным и кражу информации.

Кроме того, авторами выделяется более узкая типология киберпреступников, использующих в своей деятельности вредоносные программы («вирусы») с целью хищения денежных средств. При этом данная классификация производится по роли, выполняемой ими в слаженном многоступенчатом механизме:

а) «вирусописатель» (создатель вредоносного программного кода);

б) «заливщик» посредством рассылки спама или ссылок на сайтах распространяет вредоносную программу, тем самым способствуя ее попаданию на личные устройства пользователей;

в) «администратор» ведет интернет-ресурс, на котором содержится информация «зараженных» пользователей;

г) «дроп» обналичивает денежные средства, тем самым замыкая преступную цепочку и получая итоговые результат, на который была направлена вся деятельность преступного сообщества;

д) организатор является идейным вдохновителем и связующими элементом между всеми названными выше участниками [8, С. 26-27].

На основе изложенного выше можно сделать вывод о высокой степени разнородности

компьютерных преступников. Выделение типологии кибепреступников позволяет в дальнейшем посредством криминологического моделирования прогнозировать их возможное поведение, что в свою очередь может помочь в процессе мер, направленных на предупреждение компьютерной преступности, а также расследовании указанной категории преступлений.

Список литературы:

1. ФКУ «ГИАЦ» МВД РФ. Состояние преступности в России за январь-декабрь 2021 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 21.05.2022).

2. ФКУ «ГИАЦ» МВД РФ. Состояние преступности в России за январь-декабрь 2021 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 21.05.2022).

3. РИА Новости. В СК создали подразделение для борьбы с IT-преступлениями. [Электронный ресурс]. URL: https://turbo.ria.ru/20191219/1562589878.html (дата обращения: 21.05.2022).

4. Клещева А.С. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации // Молодой ученый. – 2018. – №37 (223). – С. 57-60.

5. Крылов В.В Информационные компьютерные преступления: Учебное и практическое пособие. – М.: Инфра-М – Норма. – 1997. – С. 285.

6. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. – Изд-во Омск. акад. МВД России. – 2009. – С. 480.

7. В. Повышев. Борьба с киберпреступностью и кибертерроризмом: доклад эксперта // Международ. Молодежная конф. Тюменская модель ООН-2012. Совет по правам человека. – 2012. – С. 18.

8. Родивилин И.П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. – 2017. – №4 (67). – С. 25-29.

9. Север Н.С. Некоторые особенности личности киберпреступников: криминологический аспект // Молодой ученый. – 2021. – №53 (395). С. 120-121.