Вероника Викторовна М.
Санкт-Петербург университет МВД России

Научный руководитель:
Пасынков Вячеслав Владимирович
Доцент кафедры криминологии
Санкт-Петербургского университета МВД России
кандидат юридических наук, доцент.

ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА

Аннотация. В данной статье приведен обобщенный анализ личности киберпреступника с учетом всех возможных факторов, влияющих на её формирование - психологических, социальных, нравственных и уголовно-правовых. Отдельного рассмотрения в рамках настоящей работы удостоен политический фактор, ставший весьма актуальным в результате жесткого противодействия, возникшего между нашим государством и недружественными странами после начала СВО. Обоснована необходимость исследования особенностей поведения киберпреступников.

Ключевые слова: *киберпреступление, киберпреступник, киберсоциум, мотивы киберпреступника. классификация киберпреступников, гибридная война.*

Введение

Актуальность разрабатываемой темы диктуется постоянно повышающимся риском для граждан, организаций и государства в целом стать объектом преступления, совершенного с

применением информационных технологий. Проблемой настоящего исследования является выявление особенностей личности преступника для полноценного принятия мер противодействия преступлениям на основе комплексного подхода.

По официальным данным МВД России, с января по декабрь 2024 года правоохранители зафиксировали 765,4 тысячи киберпреступлений. По сравнению с предыдущим годом эта цифра возросла на 23%. За пять последних лет рост составил 2,6 раза. Удельный вес в общем числе зарегистрированных преступлений превысил 40%. Как видим, IT-технологии превратились в мощный и эффективный инструмент в руках злоумышленников, совершающих свои преступления против граждан, коммерческих организаций и государственных структур. Годовой ущерб от таких преступлений превышает 200 млрд. рублей.

Перед началом исследования проблемы необходимо пояснить, какие нарушения российского Уголовного Кодекса охватываются понятием «киберпреступление». Толкование этого термина в узком смысле непосредственно связано с преступлениями, ответственность за которые предусмотрена главой 28 УК РФ «Преступления в сфере компьютерной информации». Научная литература трактует киберпреступления намного шире - как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем

или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [1, с.9]. Для достижения целей настоящей работы – исследования особенностей личности киберпреступников, их психологии и мотивов, более подходящим является широкое толкование термина «киберпреступление». Тем не менее, при использовании данного определения необходимо дифференцировать все киберпреступления на специальные, ответственность за которые предусмотрена статьями, составляющими главу 28 УК РФ, и общие, ответственность за которые определена иными нормами уголовного законодательства.

Мотивы и цели киберпреступлений

Наше исследование начнем с разборов мотивов и целей киберпреступлений, имея в виду, что каждому из возможных типов личности преступника соответствуют только ему присущие мотивы совершения преступлений. При этом, безусловно, нудно иметь в виду, что в каждом конкретном случае мотивация может быть комбинированной

Авторы работы [2], посвященной характеристикам личности интернет-преступников, придерживаются мнения, что основным мотивом киберпреступлений является ***корысть.*** По данным на 2014 год, приведенным в этой работе, раскрытые преступления в IT-сфере мотивировались корыстными побуждениями в 65% случаев. При этом 92% из выявленных преступников не были удовлетворены своим текущим материальным состоянием.

Справедливо полагая, что киберпреступления являются весьма специфической и крайне обособленной от других

направлений сферой криминальной среды, иные авторы среди мотивирующих факторов выделяют:

- ***Стремление к самоутверждению***, которого можно достичь совершением преступления высокой общественной значимости или массовости.
- ***Стремление к бескорыстному познанию*****,** двигателем которого является любопытство, исследовательский интерес и необходимость повышения собственной компетентности в IT-сфере. Например, поиск уязвимостей операционных систем или коммерческих платформ.
- ***Месть*** текущему или бывшему работодателю за несправедливое с точки зрения преступника отношение. Например, порча баз данных или организация сбоев в работе программных средств или аппаратного обеспечения работодателя. Месть может быть осуществлена и в отношении частного лица на почве личной неприязни. Месть также бывает немотивированной, основанной

на психических травмах [3] и неблагоприятной психологической обстановке, в которой пребывает преступник.

- ***Озорство***, сопровождающееся отсутствием четкой мотивации

и стремлением получить удовольствие от приведения в некомфортное состояние или неловкое положение как можно большего количества людей. Примером таких действий может служить запуск трансляций неприличного содержания на

взломанных электронных билбордах, расположенных в местах массового скопления людей.

- ***Внутренняя необходимость ощущения вседозволенности и безнаказанности,*** которую может обеспечить анонимизация преступных деяний [4] в силу свойств IT-сферы, а также возможность действовать из «информационных убежищ» вне правовой среды государства совершения преступления. Ярким примером использования такой мотивации являются хакерские группы, действующие по всему миру в интернет-пространстве с территории США и поддерживаемые АНБ и ЦРУ. Даже при раскрытии их преступлений и выявлении исполнителей, применение принципа экстерриториальности для их задержания представляется весьма проблематичным.
- ***Протестные настроения***, которые могут проявляться в виде неприятия любых видов контроля над личностью со стороны общества и государства. Причиной протестных настроений могут стать неприятие нарастания процессов общей унификации при увеличении степени цифровизации жизни, неприятие действующей политической системы, имеющегося экономического расслоения, социального и цифрового неравенства, отдельных правовых норм и правил и т.д. [5].
- ***Влияние извне,*** например, вовлечение в преступную группу, скажем, APT-группировку. Влияние извне может проявляться в виде побудительных либо принудительных действий злоумышленника на потенциального исполнителя, например, передача или обещание передачи вознаграждения за совершение

определенных действий, либо использование запугивания или шантажа.

- ***Деструктивные стремления*** [6] и социальная девиация. Такие мотивы могут присутствовать как следствие общего маргинально-нигилистского мировоззрения, в том числе под влиянием психологических состояний и психических расстройств.

- ***Политические мотивы***, возникающие на фоне внутрисистемного политического противостояния либо противостояния отдельных государств на фоне ведения гибридных войн и непосредственного вооруженного противостояния. Ярчайшим примером проявлением такой мотивации являются хакерские атаки на информационные системы России со стороны спецслужб

и отдельных исполнителей из недружественных государств, а также мошенническая деятельность враждебных колл-центров по изъятию денег у населения с целью дополнительного финансирования своих разведывательных и силовых структур, а также дестабилизации внутренней социальной, экономической и политической обстановки в нашей стране.

Способы классификации киберпреступников

Перед тем, как перейти к психологической характеристике отдельных киберпреступников, проведем их классификацию на основе разных критериев. Вначале рассмотрим способ классификации киберпреступников *по виду совершенного преступления и уровню компетентности в IT-сфере.* На основании

названных критериев преступное киберсообщество можно условно поделить на два класса.

1. ***Преступники специального киберпреступного типа.*** Представители данной категории обладают специальными техническими знаниями и навыками в определенном секторе IT – технологий. В силу того, что такие знания и навыки характеризуются высокой степенью специализации и большой глубиной проникновения в тему, его представители немногочисленны и крайне обособленны. Столь специфические признаки зачастую позволяют их обладателю ощущать себя а качестве «штучного товара» и носителя неких уникальных профессиональных тайн. Все это зачастую приводит к самоидентификации как части субкультуры «хакеров» («крекеров»), отрешенности от внешнего мира, снисходительному отношению ко всем, «кто не мы». Представители такого класса как правило, не разменяваются по мелочам и специализируются исключительно на совершении так называемых специальных киберпреступлениях, т.е. совершаемых исключительно в сфере кибертехнологий (включая программную и аппаратную составляющую).

2. ***Преступники общекиберприступного типа.*** Эта категория киберпреступников не обладают глубокими специальными знаниями в киберсфере. С помощью определенных поверхностных знаний в информационно-технической области, зачастую используя приобретенные программные и аппаратные IT-средства, такие преступники совершают неспецифические

для киберпространства деяния – кражи, обманы при помощи мошеннических схем, отмывание незаконно приобретенных денежных средств, распространение экстремистского либо иного запрещенного или ограниченно разрешенного контента (порнография, реклама табака, алкоголя, наркотиков и т.д.).

Для изучения процесса зарождения преступного умысла, его природы и степени общественной опасности, можно провести классификацию киберпреступников *по признаку степени локализации их преступной деятельности.* С этой точки зрения можно выделить три основных группы.

1. Преступники, совершающие противоправные деяния исключительно в киберпространстве. Причиной возникновения этой группы преступников являются криминогенные факторы киберпространства. К таковым можно отнести технические (наличие уязвимостей в компьютерных сетях, аппаратном и программном обеспечении), социальные (анонимность пользователей, опосредованные взаимодействия пользователей, перегрузка виртуальными социальными контактами), правовые (несовершенство законодательства и перманентное отставание в его совершенствовании от развития криминальной киберсреды) и психологические (ощущение безнаказанности, высокая степень предсказуемости последствий, комфорт места, с которого злоумышленник совершает свои действия). При ослаблении либо полном устранении каких-либо их перечисленных криминогенных факторов, такие преступники теряют свою социальную опасность.

2. Преступники, действующие как в киберпространстве, так и вне его. Преступная психология таких представителей криминального мира является преимущественно типично преступной при незначительном влиянии условий киберпространства.

3. Лица, совершившие ранее преступления, не относящиеся к разряду киберпреступлений, в последствии включивших IT – сферу в зону своих преступных интересов. Появление этой категории преступников связано с поиском преступными сообществами новых и методов деятельности. Представители этой группы киберпреступников являются организаторами преступных сообществ, используя в качестве исполнителей преступлений лиц, имеющих специальные знания и навыки в киберсфере.

Теперь перейдем к классификации, в основу которой положен психотип личности *киберпреступника,* частично пересекающийся с мотивами и целями киберпреступлений, рассмотренных выше.

1. ***Корыстный тип.*** В большинстве случаев представители этой категории ничем не отличаются от обычных преступников, главным стремлением которых является получение материальных средств противозаконным путем. При этом надо отметить, что среди преступников специального киберпреступного типа понятие корысти иногда может отличаться от обычных представлений большинства людей. Так, киберпреступники могут совершать преступления

для получения специфических предметов, имеющих особую ценность в киберпространстве, например игровых предметов, без

цели
их дальнейшей продажи.

2. ***Насильственный тип.*** К такому типу преступников относятся те, кто совершает при помощи электронных устройств и сетей такие насильственные преступления как доведение до попытки самоубийства или угроза убийством. В арсенале таких преступников - введение в заблуждение, использование неустойчивого психологического состояния или психической болезни жертвы, оскорбления и угрозы. Мотивы таких преступлений могут быть
как корыстными, когда жертва в том или ином смысле является объектом незаконного присвоения материальных или иных ценностей, так и бескорыстными, связанными с психическим либо психологическим состоянием самого преступника, либо иными мотивами, связанными с применением психологических практик, мести или далеко заходящего озорства.

3. ***Сексуальный тип.*** Для данного типа преступников характерно совершение таких преступлений, как незаконное распространение порнографических материалов или предметов без цели наживы, понуждение к действиям сексуального характера, развратные действия. В некоторых случаях совершение преступных деяний может сочетаться с насильственным типом.

4. ***Статусный тип.*** Преступники этого типа, совершая преступления, стремятся получить более высокий неформальный социальный статус в сообществах киберсоциума. В среде специального киберпреступного типа статус может иметь

достаточно серьезное мотивирующее значение, и в этом случае он тесно связан с мотивацией самоутверждения.

5. ***Исследовательский тип*** характерен для лиц, совершающих специальные киберпреступления. Мотивами для них является любопытство и стремление к бескорыстному познанию. Основой для их деятельности служит изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения. Данные цели были характерны для первых поколений немногочисленных хакеров, а также отдельных современных преступлений, хотя сейчас в большинстве случаев они выступают только дополнительным мотивом. Преступники данного типа в первую очередь направляют свои действия на устранение ошибок и развитие защиты устройств и сетей, и поэтому они могут являться условно социально «полезными». Согласно исследованию Орли Тургеман-Голдшмидт (Orly Turgeman-Goldschmidt), хакеры по-разному истолковывают свою деятельность и цели, но, тем не менее, практически все они характеризуют себя как положительных девиантов: экстраординарных людей, которые умнее других и демонстрируют необычное, лучшее поведение, или даже являются носителями социальных изменений. Одним же из главных выводов исследования было то, что хакеры не ощущают вины за собственные преступные действия [7].

6. ***Социально дезорганизующий тип***, основной целью которого является само нарушение обеспеченных законодательно социальных норм и оказание деструктивного влияния на социум и общественные отношения. Среди мотивирующих факторов таких преступников можно назвать как относительно безобидные – озорство и внутреннюю необходимость ощущения вседозволенности и безнаказанности, так и более серьезные, такие как деструктивные стремления, влияние извне и политические мотивы.

7. ***Идеологически или политически мотивированный тип.*** До начала СВО совершение специальных киберпреступлений данного типа относилось к выражению протеста во внутренней политической или идеологической борьбе. В условиях вооруженного противостояния с Западными прокси-силами и интенсификации гибридной войны во всех её видах и проявлениях, облик идеологически и политически мотивированного киберпреступника изменился коренным образом. Этот облик плавно, но неумолимо перетек из образа внутреннего диссидента во вполне сформировавшийся облик внешнего врага. Такой идеологически

и политически мотивированный тип киберпреступника воплощен в образе сотрудника иностранной спецслужбы, работающей в российском киберпространстве над дезорганизацией жизненно важных для страны цифровых платформ, связанных с госуправлением, финансами и производством, прежде всего связанным с гособоронзаказом. Еще одним значимым

направлением работы для таких киберпреступников является разведывательная деятельность на информационных ресурсах Минобороны, иных силовых ведомств и госструктур, а также осуществление промышленного шпионажа. Нанесение ущерба нашему государству враг предполагает и через осуществление мошеннических действий в отношении отдельных представителей нашего общества, наиболее уязвимых перед киберпреступностью – подростков, молодежи и людей преклонного возраста. И если пенсионеры становятся преимущественно жертвами финансового обмана, то неустоявшаяся психика и несформировавшиеся политические и жизненные взгляды подростков и молодежи становятся благоприятной средой для осуществления идеологических и физических диверсий против общества и государства.

Выводы

Для активного противостояния киберпреступности нашему научно-исследовательскому сообществу необходимо регулярно обращаться к теме киберпреступности, классификации и изучению психологии киберпреступников. Поскольку IT- сфера является одной из самых быстроразвивающихся направлений в научной, технико-технологической и общественной жизни общества и государства, то регулярное совершенствование научного и исследовательского инструментария абсолютно необходимо для того, чтобы соответствовать вызовам времени.

Список литературы

1. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. на соиск. ученой степ. канд. юрид.наук. 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Владивосток, 2005. 28 с.

2. Введенская А. Ю. Характеристика личности интернет-преступников // Журнал «Вестник Краснодарского университета МВД России», 2015.

3. Антонян Ю. М., Эминов В. Е. Преступление и наказание. Криминолого-психологический анализ: монография // Реферативный журнал «Социальные и гуманитарные науки. Отечественная
и зарубежная литература. Государство и право», 2014.

4. Мавринская Т.В., Черевиченко Т.С. Психологические особенности киберпреступников // Журнал «Инновационное развитие», 2018.

5. Пучков О. А. Мотивация действий хакеров в современной цифровой среде: междисциплинарный подход // Журнал «Проблемы современного педагогического образования», 2020.

6. Лакомов А. С. Киберпреступность: современные тенденции // Журнал «Академическая мысль», 2019.

7. Orly Turgeman-Goldschmidt. Meanings that Hackers Assign to their Being a Hacker. URL: http://www.cybercrimejournal.com/Orlyijccdec2008.

Вероника Викторовна М., 2025