Работа подготовлена с использованием системы КонсультантПлюс.

Щёлокова Ирина Алексеевна
ФГБОУВО «Российский государственный университет правосудия»
студентка 3 курса
Научный руководитель: Пискунова Е.В.

Особенности и проблемы расследования преступлений хакеров-подростков.

Начало использования термина «хакер» восходит к 1950-м годам, когда у некоторых студентов Массачусетского технологического института появилось сильное желание экспериментировать и изучать технологию. Использование термина "хакер" с годами изменилось от положительного и безобидного обозначения энтузиазма компьютерного программиста— к отрицательному и криминальному «киберпреступник», который в настоящее время является синонимом термина "хакер" и используется обычно в средствах массовой информации для обозначения злоумышленника, взломавшего компьютерные системы с целью кражи или уничтожения данных.

В 1993 году в книге "Новый словарь хакера", написанной Эриком С. Рэймондом, вводится термин «взломщик». Взломщики используют свои навыки компьютерной безопасности, связанные с авторскими вирусами, троянами и т. д., а также незаконно проникать в защищенные системы с намерением причинить вред системе или преступным намерением и отличать их от первоначального и некриминального хакера[1].

В настоящее время в интернет-пространстве также используется термин «кракер», которым обозначается именно хакеры, действующие злонамеренно, незаконно получающие доступ к учетным записям людей, злоупотребляющие защищенной информацией через сети. И рассматривая деятельность кракеров-подростков, можно сказать, что основная их масса занимается не крупномасштабными преступлениями, но тем не менее крадут информацию о кредитных картах, уничтожают важные файлы, раскрывают данные и информацию о личной жизни своей жертвы и продают их для личной выгоды.

Чтобы понять растущее преступное кибер-поведение подростков, стоит рассматривать его по отношению к обоим этим терминам.

Киберпространство образовало отдельный вид социального взаимодействия, который абсолютно не обязательно должен являться правдивым или реальным. В этом пространстве каждый может предстать в том виде, в каком хочет, сложить о себе то мнение, которое захочет и осуществить все свои нереализованные, а зачастую и корыстные, намерения.

---

[1] Jean-Loup Richet. От юных хакеров до крекеров // Международный журнал технологий и человеческого взаимодействия. — июль-сентябрь. — 2013 — С. 53.

Этот факт оказал негативное влияние на интернет-поведение современной молодёжи, которая стала использовать представляющие сами собой плюсы интернет-пространства (анонимность, уничтожение временных барьеров, многообразие форм способов связи и др.) в преступных целях.

Данная тема является очень актуальной в данный момент, так как преступность стремительно переходит в интернет-пространство. По данным МВД, в январе 2020 года зафиксировано 28,1 тыс. преступлений, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 75,2% больше, чем за такой же период прошлого года. А в общем количестве зарегистрированных преступлений их доля также значительно возросла[1].

В киберпространство переходят преступления, носящие как корыстных характер, например, взлом банковских серверов и систем, списание денежных средств с чужих банковских карт с помощью удаленного доступа, взлом банкоматов с помощью вредоносных программ, так и совершаемые на почве личной неприязни, например, кибертравля, будь то распространение личной информации или файлов, использование чужого имени, клевета или интернет-угрозы.

Можно выделить различные формы реализации таких преступлений: это могут быть преступления, совершаемые непосредственно в интернет-среде или способствующие реализации традиционных; использование информации и информационных технологий, как средства совершения преступления или неправомерные действия, направленные на изъятие, хранения или использование информации, в том числе той, которая составляет государственную или личную тайну; преступления, направленные на государственные структуры и корпорации или направленные против частных лиц или отдельных организаций и т.д.

Характер кибер-преступлений может быть разным, но ряд проблем, возникающий при их расследовании, присутствует в каждом. Так, при совершении преступлений в глобальных компьютерных сетях, их оперативно-розыскная характеристика имеет следующие сложности:

• ввиду развитых механизмов анонимности в интернет-сети, возможностей удаленного доступа и сложной организации информационного пространства высока скрытность таких преступлений, следовательно, во-первых-далеко не всегда они могут быть выявлены своевременно, во вторых- по этой причине усложняется поиск конкретных лиц, совершивших преступление. А учитывая постоянно повышающийся профессионализм субъектов данных преступлений, высокий уровень конспирации в информационном пространстве, можно сделать вывод, что кибер-преступники являются трудно-

[1] Министерство внутренних дел Российской Федерации : офиц. сайт. — Москва, 2020. — . — URL: https://мвд.рф/reports/item/19655871/.

уязвимыми для правоохранительных органов и это в совокупности обусловливает их высокую скрытность.

• трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств;

• также большую сложность составляет совершение хакерских преступных действий дистанционно, т.е. в отсутствие физического контакта злоумышленника с потерпевшим

• особая подготовленность преступников, интеллектуальный характер преступной деятельности, а также нестандартность, сложность и быстрое обновление способов совершения преступлений и применяемых специальных средств;

• невозможность предотвращения и пресечения преступлений данного вида традиционными средствами [1].

Указанные проблемы относятся как к интернет-преступности в целом, так и к преступлениям, совершаемым хакерами-подростками. При этом сложность в расследовании несовершеннолетней преступности обуславливается ещё и неодинаковостью самого понятия «совершеннолетие» в различных государствах. Так, например, совершеннолетними в Южной Корее и Японии считаются лица, достигшие 20 лет, в Алжире и Шотландии-достигшие 19 лет, а в Ливии, Боливии и Аргентине-21 года. Также есть и государства, еде установлен различный возраст даже в разных частях страны, например, в большинстве штатов США лица достигают совершеннолетия в 18 лет, но в Вайоминге, Алабаме и Небраске – этот возраст составляет 19 лет, а в Миссисипи и штате Нью-Йорк – 21 год.

Основной упор в расследовании данной группы преступлений ранее делался на сами компьютерные технологии (отслеживание IP-адреса и выявление конкретного компьютера, с помощью которого было совершено преступление, исследование вредоносного программного обеспечения), что повлекло активное развитие судебных компьютерных экспертиз. Однако в последнее время появились исследования, направленные на изучение личности киберпреступников и отдельного внимания заслуживают подростки, что является весьма целесообразным направлением. С одной стороны, потому что осведомленность и «продвинутость» нынешнего поколения в инновациях и всевозможных хитростях интернетпространства позволяет им использовать и создавать более изощренные, быстрые и ловкие методы хакерских атак. С другой стороны, потому что и без того сложный процесс расследования преступлений международного характера в данном случае усложняется ещё и спецификой несовершеннолетнего субъекта.

[1] Осипенко А.Л. Сетевая компьютерная преступность. Омск, 2009.

Субкультура хакеров, которая влияет на все сетевое общество, формирует определенную систему ценностей и особое восприятие мира, где государству отводится роль противника, врага. Общество в «хакерской» трактовке-«слепое стадо», а преступление-способ возвышения над обществом и государством. Это служит легитимации противоправной деятельности, как в восприятии самих хакеров, так и в восприятии общества1.
По отношению к подросткам этот факт проявляется наиболее явно, так как большинство из них недополучают должного внимания в детстве или ограничены в выборе организации своего досуга, ввиду чего формируется важная особенность культуры юных хакеров-представление о собственной избранности, элитарности. Многие из них оценивали себя как первопроходцев, создающих новое общество, основанное на ценностях глобального киберпространства.

Уровень таких преступлений обуславливает комплекс причин воспитательного и информационно-технологического характера, например, такие как: неконтролируемая виртуальная паутина; высокая безработица, низкий уровень жизни населения, отсутствие должного контроля за подростками, бездействие образовательных учреждений и государства в целом в совершенствовании методов противодействия преступлениям в сети Интернет, отсутствие четкого алгоритма действия по выявлению киберпреступности в глобальной сети, отсутствие контроля со стороны родителей за времяпрепровождением ребенка.

Преступность в подростковом возрасте отличается тем, что несовершеннолетние в большинстве случаев совершают свои деяния, не задумываясь о последствиях. Как правило, ими руководит внезапно появившееся и быстро проходящее влечение к какому-либо объекту. Совершая компьютерные преступления, подростки редко руководствуются корыстными мотивами, в большинстве случаев они просто желают произвести впечатление на своих друзей и бросить вызов политической системе, юными хакерами движет преданность своим идеалам и желание впечатлить знакомых, а не жажда наживы. А при совершении, в частности, кибертравли преобладающим руководящим мотивом является личная неприязнь, так как травле, в основном, подвергаются знакомые преступнику лица, что обуславливается импульсивностью подростков, их юношеским максимализмом и, опять-таки, желанием стать лидером компании и заработать авторитет.

Проблемы выявления и расследования преступлений хакеров подростков можно поделить на проблемы, связанные с международно-правовым регулированием и взаимодействием и собственно криминалистические. К

---

[1] Дремлюга Р.И. Субкультура хакеров и другие факторы компьютерной преступности // Криминологический журнал байкальского государственного университета экономики и права. — 2008 — С.22.

первым, условно, можно отнести преступления, совершаемые напрямую против иностранных граждан или структур, находящихся на территории другого государства (экономические преступления против средств иностранных граждан и организаций, взлом иностранных структур и баз данных и т.д.), и преступлений, совершаемых в пределах одного государства, но тем не менее затрагивающих международные интересы и безопасность (экстремизм, преступные операции с банкоматами, списывание денежных средств с чужих сетов, мошенничество и т.д.).

При расследовании данных преступлений, стоит задаться вопросом о допустимости применяемых для этого методов, так как органы власти сами могут в этой ситуации стать субъектами нарушения законодательства. Так при расследовании первой категории преступлений государства зачастую способны выходить за пределы своей юрисдикции и нарушать тем самым суверенитет и законодательство других государств. В другом случае речь идет о возможности государства осуществлять юрисдикцию над гражданами в пределах своего государства, не нарушая их личного пространства и не прибегая к несанкционированному доступу к их данным. А говоря о несовершеннолетних, как о субъектах совершения таких преступлений, серьезной проблемой международного характера является различие в возрасте привлечения к уголовной ответственности в разных странах, о чем уже упоминалось в статье.

К собственно криминалистическим же относятся трудности, связанные, например, с отслеживанием технических средств, с помощью которых было совершено преступление, поиском самих хакеров-подростков, производством компьютерных экспертиз. Последние характеризуются тем, что в возможности компьютерной экспертизы не входит определения лица, совершившего преступление, а лишь установление технического средства или его местонахождение. И здесь появляется ещё одна проблема: при совершении одного компьютерного преступления, например, неправомерного доступа к компьютерной информации, может быть несколько мест происшествия: рабочее место, где обрабатывается информация, ставшая предметом преступного посягательства; место, где информация хранится; место осуществления неправомерного доступа к компьютерной информации, например, при взломе путем внешнего сетевого удаленного доступа; в ряде случает также место, где происходило создании программы взлома, подбирались пароли и место непосредственного использования или распространения информации[1].

Ещё одним фактором, затрудняющим расследование указанных деяний, является недостаточно эффективная деятельность правоохранительных органов: недостаточная квалификация сотрудников оперативных

[1] Ишмаева Т. П. К вопросу об особенностях осмотра места происшествия по делам о компьютерных преступлениях // Журнал «правопорядок: история, теория, практика» — №4 (7). — 2015 — С. 38-42.

подразделений ОВД; отсутствие научных разработок и методик по использованию всего спектра кибер-розыскной работы в этом направлении; недостаточно эффективное взаимодействие как между субъектами оперативно-розыскной деятельности, так и международного сотрудничества в сфере ОРД.

Учитывая тот факт, что в противоправных деяниях хакеров, и в частности хакеров-подростков, активизировалась транснациональная и международная составляющая, а борьба с преступностью в области межнациональных компьютерных сетей усложняется для противоправной деятельности как отдельными лицами, так и преступными группами, необходимо постоянное международное сотрудничество, так как контролировать данный вид преступности и бороться с ней на уровне отдельного государства практически невозможно.