УДК 343.918.1

Типы компьютерных мошенников

Гайфутдинов Р.Р.
Ассистент кафедры уголовного права
Казанского (Приволжского) федерального университета

В статье рассматриваются криминологические вопросы изучения компьютерных мошенников как одного из видов компьютерных преступников. Автором поставлена цель классифицировать компьютерных мошенников для дальнейшего изучения причинных комплексов, детерминирующих преступность. Результатом проведенного исследования стала классификация компьютерных мошенников на традиционных и профессиональных с последующим их делением на виды по специализации преступной деятельности. Полученные данные об особенностях преступной деятельности и личности преступников станут базой для разработки программы по борьбе с компьютерной преступностью.

Ключевые слова: компьютерная преступность, компьютерные преступления, киберпреступность, компьютерное мошенничество, преступность в сфере компьютерной информации, личность компьютерного преступника.

Компьютерные технологии прогрессивно развиваются с каждым годом, а российский сегмент информационно-телекоммуникационный сети Интернет является самым активным и самым растущим сегментом экономики страны, который все больше влияет на другие отрасли. Объем экономики Рунета по состоянию на 2015 г. составляет 1,4 трлн. руб., 0,6 млрд. руб. из которых составляет рынок онлайн-платежей, а вклад в ВВП страны оценивается в 2,4 % от его общего показателя [1, с. 7].

Такое положение естественным образом обуславливает появление новых форм и видов компьютерной преступности, в том числе компьютерных мошенничеств. В специальной литературе авторами приводятся различные типы личности компьютерных преступников. Среди таких работ важно отметить труды А.А. Жмыхова [2, с. 57-58], А.А. Простосердова [3, с. 165], В.Б. Вехова [4, с. 31-36], Т.М. Лопатиной [5, с. 30-31], А.Э. Побегайло [6, с. 35], Р.И. Дремлюги [7, с. 143], М.Ю. Батурина [8, с. 27-34], М.Ю. Дворецкого, А.Н. Копырюлина [9, с. 172] и др. Однако, в литературе мало изучен вопрос классификации компьютерных мошенников, являющихся одним из видов компьютерных преступников.

В данной работе уделено минимальное внимание способам совершения компьютерных мошенничеств, вместе с тем обойтись без их краткого рассмотрения невозможно для уяснения специфики действий компьютерного преступника, из которой впоследствии и раскрываются личностные особенности преступника.

В современном обществе умение пользоваться компьютерной техникой уже не считается специальным знанием. Поэтому лиц, использующих для мошенничества телефоны, компьютеры и другую высокотехнологическую технику (традиционных компьютерных мошенников), необходимо отличать от мошенников, высокотехнологические средства в деятельности которых играют особую роль и становятся необходимой составляющей в их преступной деятельности (профессиональных компьютерных мошенников).

Среди регистрируемой компьютерной преступности традиционные виды компьютерного мошенничества составляют большую долю преступлений в отличие от профессиональной. Правоохранительные органы осуществляют борьбу с традиционными компьютерными мошенниками путём активного информирования граждан о способах и методах мошенничества. Традиционные компьютерные мошенники в своей преступной деятельности используют давно известные способы, которые реализуются посредством компьютерных технологий: сообщение о выигрыше приза, уведомление о получении наследства, запрос на покупку, продажу или иные операции с недвижимостью или ценными бумагами, просьба об оказании финансовой консультации или помощи, виртуальные знакомства, требование выкупа и др.

Такие способы мошенничества являются распространёнными во многих развитых зарубежных государствах. Так, согласно отчета Australian Institute of Criminology, составленного за 2014 г., 98 % из опрашиваемых респондентов получали сообщения мошеннического предложения за последние 12 месяцев [11]. Преступный охват мошенниками населения поражает.

Традиционные способы компьютерного мошенничества не отличаются тщательным планированием, рассчитаны на массового «дурака» в отличие от преступлений, совершаемых профессиональными компьютерными мошенниками.

В литературе «под профессиональной преступностью понимается одна из форм преступной деятельности, которая характеризуется как промысел, являющийся для преступника основным источником дохода и требующий специальных знаний, навыков и умений» [12, с. 242].

Среди признаков профессиональной преступной деятельности называют: постоянство и регулярность криминальной активности, наличие специализации и навыков преступного ремесла, закрытость от общества, высокая степень защиты от уголовного преследования, структурная иерархичность и существование в рамках особой криминальной субкультуры. Они также свойственны компьютерным мошенникам и будут рассмотрены при характеристике каждого из видов.

Профессиональных компьютерных мошенников можно разделить на кардеров (стафферов, заливщиков, дроповодов и др.) и фишеров.

Кардеры (словообразование от англ. *card* – кредитная карточка) – лица, незаконно использующие принадлежащую третьим лицам информацию о платежных средствах. В соответствии с их более узкой специализацией в преступной деятельности среди кардеров особо выделяются следующие виды.

Стафферы (производное в пер. с англ. *stuff* – вещь) или вещевики. Деятельность стафферов связана с хищением товарно-материальных ценностей посредством использования платежных средств, позволяющих производить расчеты дистанционным способом, в интернет-магазинах, на аукционах и в других организациях, осуществляющих товарооборот посредством информационно-телекоммуникационной сети Интернет. Например, это может быть покупка вещи в интернет-магазине с использованием сведений о банковской карте третьего лица.

Заказы могут оформляться на лиц, которым не известно о противоправности осуществляемого заказа. Такие лица называются дропами (словообразование от англ. *drop*, в пер. – бросать, кидать).

Приискание дропов осуществляется дроповодами. Дропы, которым предлагается работа по приему и пересылке похищенного имущества, зачастую становятся жертвами обмана.

В процессе приискания дропов осуществляется их мощная психологическая обработка, в которой значительное влияние оказывают языковые знания на уровне их носителей, правовой регламентации деятельности организации, на чьей территории осуществляется их приискание. Всё перечисленное направлено на то, чтобы предлагаемая работа выглядела как можно легальнее по всем своим признакам.

Лицам, ищущим вакансии, зачастую рассылаются предложения о работе, в которой необходимо принять на свое имя денежные средства и далее перечислить их на счета третьих лиц. В таких случаях лица становятся дропами в противоправной деятельности так называемых заливщиков.

Современные платежные системы предпринимают как можно больше средств защиты своих клиентов от компьютерных мошенников: подтверждение личности путем звонка (опрос личных данных владельца средства платежа), направление кода верификации через SMS и др.

Заливщики профессионально преодолевают такие средства банковской безопасности: предварительно осуществляют максимально возможный сбор данных для доступа посредством сети Интернет к средствам платежа жертв и последующего подтверждения денежного перевода. Сбору персональных данных о владельце платежного средства иногда способствуют интернет-сервисы, предоставляющие на возмездной основе персональные данные о лицах. Некоторые из таких сервисов используются работодателями для проверки претендентов на вакантные должности.

Фишеры (производное от англ. слова *phishing*: *password* – пароль; *fishing* – рыбная ловля) – это лица, осуществляющие сбор конфиденциальных данных о платежных средствах путем обмана пользователей. Фишерами рассылаются сообщения, содержащие ссылки на сайт организации, от имени которой они представляются, внешне только с ней схожей, на котором побуждают жертву ввести информацию о доступе к онлайн-банкингу, свои персональные данные и другие конфиденциальные сведения.

Профессиональные фишеры обладают психологическими приемами, которые могут воздействовать на сознание человека удаленно, что является непростой задачей. Таким образом, жертва, только прочитав сообщение, должна под воздействием одного текста совершить необходимое для фишера действие. У компьютерных мошенников нет в арсенале иных способов воздействия на жертву через другие органы восприятия информации. Положительный эффект для фишера зачастую достигается посредством массовости его действий.

Профессиональная компьютерная преступность в сети Интернет имеет свою специфику.

Общество компьютерных мошенников устоялось как некая субкультура, которой присуща массовая численность, устойчивость взглядов, выработанность норм и правил поведения в интернет-пространстве. Интернет-ресурсы, посвящённые тематике компьютерного мошенничества, ранее были совмещены с ресурсами хакерской тематики. Если раньше такие ресурсы были в открытом доступе, то в настоящее время их публичная деятельность не практикуется, почти все профессиональные форумы носят закрытый характер. При излишнем привлечении каким-либо форумом внимания со стороны правоохранительных органов или общественности к своей деятельности, администрация переводит форум на другое доменное имя. Компьютерные мошенники в конспирологических целях меняют место дислокации своих площадок, на которых они делятся опытом и осуществляют разработку новых способов преступной деятельности.

В целях конспирации своей деятельности на многих из них была закрыта свободная регистрация. Лицо, желающие принять участие в обсуждении способов преступной деятельности, накоплении новых знаний, приискании соучастников, должно заплатить определённую плату.

Площадки для общения компьютерных мошенников образуют сложную социальную структуру в целях организации обмена опытом, координации деятельности, торговли и др. Так, если это форум, то здесь может присутствовать его администратор (*admin*), технический помощник (*technical support*), помощник по общим вопросам и регистрации (support), модераторы разделов, являющиеся специалистами в соответствующих областях (*moderator*), проверенные продавцы (*vendor*), почетные либо особо отличившиеся члены преступного общества (VIP) и т.д.

Наличие особой субкультуры компьютерных мошенников обосновывается тем, что осуществляется производство кинофильмов, посвящённых такой преступной деятельности, которая общественностью не осуждается [13].

На закрытых площадках выработаны неформальные нормы и правила поведения. Например, не приветствуются знакомства в реальной жизни, не принято задавать вопросы личного характера, которые могут способствовать раскрытию личности преступника. Некоторые профессиональные компьютерные мошенники следуют правилу – не действовать против интересов Российской Федерации.

В психологии профессиональных компьютерных мошенников есть одно существенное различие с хакерами: им не свойственно себя делить на законопослушных лиц (так называемых вайтхатов) и незаконопослушных. Если некоторым хакерам тяжело переступить в себе нравственно-воспитательную установку для совершения противоправных деяний (украсть деньги с банковского счета, кого-то обмануть), то кардерам, напротив, свойственно оправдывать себя тем, что они не являются преступниками в связи с тем, что не совершают общеуголовных преступлений. В общественном сознании не переломлен психологический барьер, который не относит лиц, совершающих необщеуголовные преступления, к преступникам. Некоторые компьютерные мошенники убеждены, что приносят пользу, совершая хищения в США и других европейских странах.

С профессиональной точки зрения, кардер – человек с высоким уровнем интеллекта, знающий в совершенстве один или несколько иностранных языков. Многие кардеры активно применяют средства шифрования для сокрытия своей личности, а также активно их совершенствуют. Так, ими используются шифрованные каналы передачи данных (напр., *Tor*) и бесконтрольные со стороны государства финансовые структуры для взаимодействия (напр., *Bitcoin*).

В реальной жизни у кардеров, очевидно, возникают трудности в обосновании своих преступных доходов: им свойственно оправдываться легальными источниками доходов в интернет-пространстве, например, выдавать себя за программистов.

Кардерам присуща преступная деятельность в мультигеографическом масштабе, это объясняется конспирологической возможностью быть вне зоны досягаемости спецслужб стран, против экономических интересов которых осуществляется их деятельность. Глобализация платежных систем предоставляет преступникам возможность похищать данные пользователей банковских счетов, например, в США, а обналичивать деньги с этих счетов в других, более «безопасных» для деятельности кардеров, государствах.

Следующая важная особенность российских кардеров: осуществление преступной деятельности в ночное время суток. Она объясняется режимом работы интернет-магазинов, банковских и иных коммерческих структур зарубежных государств. Таким образом, кардеры синхронизируются со временем деятельности организаций, в которых совершают хищения.

На фоне «ночной» деятельности проявляются некоторые психологические особенности личности. Интернет, в отсутствие постоянного места официальной работы, для компьютерных мошенников является средой обитания. Как отмечается исследователями, у таких лиц есть склонность к развитию интернет-зависимости [10, с. 102], в СМИ также есть упоминания о болезни киберпреступников Адриана Ламо и Райана Клири синдромом Аспергера – одной из форм аутизма, характеризующейся трудностями в социальном взаимодействии [14].

Переход с одной узкой преступной специализации на другую является иногда весьма затруднительным: для освоения новых способов преступной деятельности необходим опыт, который находится в тесной зависимости с потраченным на него временем, в течение которого необходимо осваивать специфические знания. Поэтому распространяется такое явление, как оборот преступных схем в сети Интернет, методических пособий для компьютерных мошенников.

Компьютерным мошенникам присуща тенденция к организации устойчивых преступных групп транснационального характера. Компьютерных мошенников-одиночек становится все меньше. Большинство способов компьютерного мошенничества невозможно исполнить одному либо они нерентабельны.

Преступная группа может состоять из «вбивалы», который приобретет информацию о банковском счете и оформит денежный перевод в банке, «прозвонщика», который позвонит в банк и подтвердит денежный перевод, дропа, который получит денежные средства на свой счет и перечислит их, и «обнальщика», который обналичит денежные средства и переведет на другой счет.

Вместе с названными типами профессиональных преступников существуют смежные и иные типы компьютерных преступников. Такие типы могут также появляться ввиду совершенствования и изобретения новых преступных способов.

Сегодня экспертами в сфере информационной безопасности немало говорится о проблемах выявления, раскрытия и привлечения к уголовной ответственности компьютерных мошенников. На наш взгляд, указанные проблемы кроются в попустительской политике государства при внутренних посягательствах и отсутствии соответствующих международных и межгосударственных соглашений по вопросам взаимодействия при транснациональном характере действий преступников. Кроме того, сфера виртуальной жизни отличается от реальной легкостью сокрытия своей личности, она в меньшей степени контролируется государством, что способствует распространению компьютерного мошенничества. Обозначенные нами проблемы являются важными причинами самодетерминации компьютерных преступлений.

Вместе с тем остаётся очевидной необходимость дальнейшего тщательного изучения причинного комплекса факторов, детерминирующих компьютерную преступность мошенников и личности компьютерного преступника, для выработки общих рекомендаций и составления планы борьбы с преступностью.

Литература:

1. Плуготаренко С. Влияние Рунета на экономику // Тематическое приложение к ежедневное деловой газете РБК. – 2017. – № 069 (2566).
2. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук. – М., 2003. – 178 с.
3. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. – М., 2016. – 232 с.
4. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования / Под ред. акад. Б.П. Смагоринского – М.: Право и Закон, 1996. – 182 с.
5. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. ... доктора юрид. наук.: – М., 2006. – 60 с.
6. Побегайло А.Э. Киберпреступность: лекция. – М.: Акад. ГП РФ, 2013. – 50 с.
7. Дремлюга Р.И. Интернет-преступность: дис. ... канд. юрид. наук. – Владивосток, 2007. – 248 с.
8. Батурин Ю.М. Право и политика в компьютерном круге. – М.: Наука, 1987. – 112 с.
9. Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. – Тамбов: ТГУ им. Г. Р. Державина, 2006. – 212 с.
10. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. … канд. юрид. наук. – Пятигорск, 2010. – 262 с.

11. Jorna P. Australian Institute of Criminology. Australasian Consumer Fraud Taskforce: Results of the 2014 online consumer fraud survey [online]. – Canberra, ACT: Australian Institute of Criminology, 2016. – URL: http://aic.gov.au/media_library/publications/rr/001/rr001.pdf, свободный. – Проверено 25.04.2017.
12. Криминология: учеб. / И.Я. Козаченко, К.В. Корсаков. – М.: Норма: ИНФРА-М, 2011. – 304 с.
13. Голованов В. Blackhat – новый блокбастер, пытающийся реалистично показать работу хакеров // Geektimes – 2015. – 19 янв. – URL: https://geektimes.ru/post/244498/, свободный. – Проверено 25.04.2017.
14. Chidambaram V. The Profile of a Cyber Criminal // PC Advisor – 2012. – 13 янв. – URL: http://www.pcadvisor.co.uk/feature/security/profile-of-cyber-criminal-3330068/ The Profile of a Cyber Criminal, свободный. – Проверено 25.04.2017.

Types of Computer Fraudsters

R.R. Gayfutdinov
Kazan (Volga Region) Federal University

The article is devoted to topical questions of computer fraudsters as one of the types of computer criminals. The author classified computer fraudsters in order to reveal determinants of crime aimed at their further research. As a result, the computer fraudsters were categorized into traditional and professional computer fraudsters with their further subdivision based on types of their criminal activities, which could then serve as a basis for the development of programs to combat this type of crime.

Key words: computer crime, computer criminal, cybercriminal, types of computer criminals, crimes in the sphere of computer information, professional criminal, computer fraud, the personality of computer criminal.

◆