УДК 343.918.1

К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности

Гайфутдинов Рамиль Рустамович

Ассистент,
кафедра уголовного права,
Казанский (Приволжский) федеральный университет,
420008, Российская Федерация, Республика Татарстан, Казань, ул. Кремлевская, 18;
e-mail: gayfutdinov.r@yandex.ru

Аннотация

Целью работы является изучение личности отдельных категорий компьютерных преступников с учетом распространенности существующий наименований. За основу предлагаемой типологии личности компьютерного преступника приняты специфические черты того вида преступной деятельности, которые изложены в соответствующих статьях Уголовного кодекса Российской Федерации. Представляется, что в способе реализации преступной деятельности компьютерного преступника раскрываются определенные личностные особенности самого субъекта преступления. По результатам проведенного исследования получены новые выводы об особенностях социального портрета личностей, совершающих киберпреступления. Уточненная типизация компьютерных преступников способствует установлению подлинного смысла и содержания состава преступления, определению соответсвующего наказания и разработке мер предупреждения преступности в сфере компьютерной информации.

Для цитирования в научных исследованиях

Гайфутдинов Р.Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. 2017. Том 7. № 4А. С. 245-256.

Ключевые слова

Компьютерная преступность, компьютерные преступления, личность компьютерного преступника, типология личности компьютерного преступника.

Введение

Согласно экспертным данным в мире ежегодно наблюдается рост компьютерной преступности и произведенного ущерба [Лацинская, 2016, www]. Центральный банк Российской Федерации сообщает, что банки и их клиенты понесли убытки в размере около 2 млрд. руб. в результате хакерских атак за 2016 год [Прокофьев, 2016, www]. Указом Президента Российской Федерации В.В. Путина 5 декабря 2016 года утверждена новая Доктрина информационной безопасности Российской Федерации, в которой подчеркнуто, что в настоящее время возрастают масштабы компьютерной преступности, при этом методы, способы и средства совершения таких преступлений становятся все изощреннее. Поэтому в Российской Федерации особую актуальность приобретает изучение не только технических, политических, социологических и экономических, но и правовых (юридических) аспектов преступности в сфере компьютерной информации в целях обеспечения информационной безопасности, являющейся составной частью национальной безопасности Российской Федерации.

Уголовный кодекс Российской Федерации (далее – УК РФ) предусматривает достаточно строгие меры ответственности за неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационной сетей (ст. 274).

Каждый из названных видов уголовно-наказуемой компьютерной деятельности имеет свою специфику, которую уголовный закон отражает главным образом в объективных признаках соответствующих составов преступлений. Представляется, что характер совершаемых деяний в определенной степени отражает и тип личности самого преступника. С другой стороны, проблема изучения личности преступника, их типологии может представлять важное значение как для квалификации преступлений, определения вида и меры наказания, так и для разработки мер предупреждения компьютерной преступности.

Личность компьютерного преступника и характер совершаемого им преступления

Характеристика особенностей и типология личности компьютерного преступника позволяет акцентировать внимание не только на общих чертах (свойствах), сходных с иными категориями преступников, но и на специфике личности данной категории преступников. Общепризнанные положения теории личности преступника увязывают некоторым образом тип личности с определенными способами ее проявления. В литературе отмечается, что характер самого преступления или тип криминальной направленности личности преступника может быть самостоятельным *основанием* типологии [Лейкина, 1968, 32].

Для сферы компьютерной преступности это предложение представляется весьма актуальным. Например, неправомерный *доступ* к компьютерной информации (ст. 272 УК РФ) существенно отличается от деятельности, именуемой в законе *созданием* компьютерных программ (ст. 273 УК РФ), не только по объективным признакам соответствующего состава преступления, но, в известной степени, по некоторым свойствам и компетенциям личности самого деятеля. В специальной литературе обычно выделяются «хакеры»[1], «вирусмейкеры»[2] и другие типы субъектов, выполняющих существенно отличающиеся друг от друга виды деятельности.

Важно также учитывать, что по содержанию субъективных признаков составы преступлений в сфере компьютерной информации могут быть связаны с определенным видом мотивации (например, корыстная заинтересованность). В то же время основные составы, предусмотренные в соответствующих статьях, обычно не содержат указания на мотив. Следовательно, законодатель допускает совершение предусмотренных ими деяний при наличии *любого* мотива, а корыстная заинтересованность является признаком квалифицированного состава (см., напр., часть 2 ст. 272, 273 УК РФ). Известно, что установление мотивов совершения преступления имеет важное значение для решения вопросов квалификации преступлений, назначения наказания и профилактики компьютерной преступности. Поэтому при рассмотрении типовых особенностей личности преступников в сфере компьютерной информации важно иметь в виду их мотивационную составляющую.

Применительно к типизации компьютерных преступников предлагаются следующие основания (критерии). Так, А.А. Жмыхов разделяет их на два типа: традиционный общеуголовный преступник и хакер. При этом под традиционным общеуголовным компьютерным понимаются мошенники, вандалы, воры, вымогатели, террористы, с присущими им специфическими чертами, которые отличают их от иных общеуголовных элементов. Хакером именуется компьютерный пользователь, который незаконно обретает доступ к средствам компьютерной техники и данным в совокупности с их несанкционированным использованием [Жмыхов, 2003, 57-58].

Следует подчеркнуть, что в отечественной и зарубежной литературе утвердилось и другое наименование компьютерного преступника – киберпреступник. С учетом этого А.А. Простосердов разделяет киберпреступников на традиционных киберпреступников и хакеров [Простосердов, 2016, 165]. Р.И. Дремлюга делит их на интернет-мошенников, интернет-взломщиков (хакеров) и создателей Интернет-вирусов [Дремлюга, 2007, 143]. Другие авторы подразделяют лиц, совершивших компьютерные преступления, по иным критериям: фанатики (лица, отличительной особенностью которых является устойчивое сочетание профессионализма с элементами своеобразного фанатизма и изобретательности), психически больные лица (страдающие информационными болезнями или компьютерными

1 От англ. hacker, что дословно означает «рубщик».
2 Словообразование от англ. слов virus maker дословно означающих «создатели вирусов».

фобиями) и профи (профессиональные компьютерные преступники) [Вехов, 1996, 31-36; Лопатина, 2006, 30-31; Побегайло, 2013, 35]. М.Ю. Батурин, в свою очередь, подразделяет компьютерных преступников по признакам субъективной стороны преступления: корыстные преступники; лица, совершившие компьютерные преступления по небрежности. Кроме того, среди компьютерных преступников он особо выделяет шпионов, хакеров (взломщиков) и кракеров (компьютерных хулиганов) [Батурин, 1987, 27-34]. Несколько иные критерии выдвигают М.Ю. Дворецкий и А.Н. Копырюлин. Они подразделяют компьютерных преступников на следующие группы: нарушители правил пользования ЭВМ, «белые воротнички» (или респектабельные преступники), компьютерные шпионы и хакеры [Дворецкий, 2006, 172]. Кроме того, по критерию возможности доступа к информации А.Н. Копырюлин разделил компьютерных преступников на внутренних и внешних нарушителей [Копырюлин, 2007, 171]. Сара Лоуман также обособила преступников, действующих изнутри компании (работники, консультанты, временные помощники организации), от иных компьютерных преступников. В последующем она выделила среди них шпионов, саботажников и похитителей личных данных [Lowman, 2010, www].

С учетом положений действующего УК РФ вполне приемлемой при изучении личности компьютерных преступников является также типология на основе специфики *объективной стороны* их *деятельности* в сочетании с *субъективными* ее составляющими. Так, опираясь на положения УК РФ, преступников в сфере компьютерной информации можно, в первую очередь, подразделить на лиц, осуществляющих неправомерный *доступ* к охраняемой законом информации (ст. 272 УК РФ), и на лиц, *создающих, распространяющих или использующих*, компьютерную информацию для целей, указанных в законе (ст. 273 УК РФ). Каждому из названных видов преступной деятельности может соответствовать определенный тип личности преступника, располагающего особой совокупностью компетенций, мотивацией и целеполаганием. Компьютерные преступники соответствующего типа при посягательстве на охраняемые законом интересы могут причинять вред, действуя как извне, так и изнутри самой организации.

В специальной литературе используется особая терминология для характеристики каждого из разновидностей (типов) лиц, совершающих определенные *виды неправомерных* действий в сфере компьютерной информации. При этом такие характеристики, конечно, не всегда могут быть востребованы в полной мере для решения ряда уголовно-правовых и криминологических вопросов, однако такие оценки представляют определенный интерес.

Хакер как личность и субъект преступления

Так, лиц, осуществляющих неправомерный *доступ* к охраняемой законом компьютерной информации, обычно именуют **хакерами**. Хакеры оказали значительное влияние на

формирование целой субкультуры со своими представлениями о содержании отношений к системе социальных ценностей. В литературе нередко утверждается, что сложилась определенная молодежная субкультура хакеров, которая способна влиять на систему целеполагания своих сторонников и формирование мотивов совершения компьютерных преступлений [Дремлюга, 2008, 142]. При этом для хакеров достаточно важным является сам факт причисления себя к этой субкультуре.

Располагая относительно высоким интеллектом, наличием определенных компетенций, склонностью к неординарным формам реакции на социальные катаклизмы, эти лица подчас испытывают известное внутреннее желание преодолевать свойственное многим из них элементы социального отчуждения, настоятельную потребность в демонстрации своей социальной значимости для близкого окружения и общества в целом.

Личность хакера, как субъекта, принадлежащего к иной части социума, средствами массовой информации и киноиндустрией не всегда характеризуется однозначно. При этом не исключается представление о хакере как лице, выполняющим не только социальные функции, но и реализующем запросы общества, а, возможно, и политические интересы, связанные с заданиями органов государства либо определенных его структур. В соответствии с этим им пытаются подражать другие, стремящиеся начать «карьеру» компьютерного деятеля, пробующие свои возможности в этой компьютерной сфере. Хотя хакеры в основном являются преступниками одиночками, им свойственно хвастаться своими достижениями и обсуждать их [Дворецкий, 2003, 159].

Хакеры разительно отличаются от других типов компьютерных преступников своими профессиональными знаниями и навыками, которые, в то же время, требуют постоянного совершенствования в силу перманентного укрепления, совершенствования средств защиты компьютерной информации. Они располагают специфическим инструментарием и знанием компьютерной техники, причем не только технической или аппаратной их части. Чаще всего эти лица являются также профессионалами в области программирования таких систем. Иным типам компьютерных преступников эта область знаний свойственна лишь на некотором минимальном уровне либо такие компетенции могут быть им не свойственны вообще, что определяет *иную сферу* их уголовно-наказуемой деятельности.

Используемый хакерами инструментарий в неправомерной деятельности зависит не только от его доступности, но и также определяется личными предпочтениями преступников: некоторые принципиально не используют какое-либо программное обеспечение (напр., продукцию Microsoft), другие, в силу наличия «любимых» языков программирования, используют программное обеспечение, написанное на этом языке. Кому-то из хакеров присущи любимые способы или методы получения неправомерного доступа (напр., атаки типа SQL, XSS-инъекций, и т. д.). Таким образом, характер этих предпочтений в некоторой степени можно увязать и с особенностями личности хакера.

В отличие от других компьютерных преступников хакеры предпочитают также быть менее зависимыми от своей команды. Некоторые компьютерные преступники в силу имеющихся профессиональных навыков и способностей обеспечивают других сведениями для осуществления ими своей дальнейшей деятельности. К примеру, известно, что некоторые хакеры практикуют обеспечение кардеров[3] сведениями о банковских счетах.

Отдельным категориям хакеров трудно переломить в себе сформулированную ранее нравственно-воспитательную установку, препятствующую совершению преступных деяний корыстной направленности: к примеру, совершать хищения с банковских счетов. Обращает на себя внимание то, что хакеры, обычно признавая необходимость существование закона, осознавая справедливость и гуманность многих охраняемых законом положений, считают при этом, что нарушение требований закона может иметь место только в «реальной» жизни. Поэтому полное погружение в виртуальное пространство позволяет им противопоставлять его «реальной» жизни. В связи с этим некоторые авторы убеждены в том, что у хакеров искажен элемент правосознания, отвечающий за личное исполнение правовых предписаний [Евдокимов, 2006, 142]. Отмеченное не исключает того, что умышленные действия, заключающиеся в неправомерном доступе, могут сочетаться с легкомысленным или небрежным отношением к обозначенным в законе преступным последствиям (вреду).

Среди хакеров есть специалисты в узких, излюбленных ими областях. По этому основанию и с учетом сферы деятельности их можно разделить на подвиды: фрикеров[4], кибертеррористов и крэкеров[5].

Принято считать, что *фрикинг* предшествовал хакерской субкультуре. Фрикеры с середины XX века осуществляли взлом телефонных сетей поначалу для получения возможности бесплатных звонков. Сейчас фрикерами называют лиц, получающих неправомерный доступ к системам защиты охранных систем (например, помещений, хранилищ, транспортных средств), ТВ, радио, спутниковых систем связи и др.

Некоторые авторы относят фрикеров к мошенникам в сети Интернет [Комаров, 2010, 64]. Дело в том, что в недавнем прошлом фрикеры для неправомерного доступа к системам использовали среди прочих методы социальной инженерии. Нам представляется, что этот вариант типизации спорный, а его обоснование – небезукоризненным.

Кибертеррористы – хакеры, специализирующиеся на промышленном шпионаже, кибердиверсиях (саботаже) и действующие главным образом против правительственных структур, специальных служб и организаций, обладающих социально значимой

3 Мошенники, использующие поддельную или принадлежащую другому лицу платежную карту или сведения о банковском счете (от англ. card – платежная карта).

4 От англ. phreaking (phone и freak, в переводе означающие «телефон» и «фрик»).

5 От англ. crackers, что дословно означает «растрескиватели».

информацией. Одним из способов совершения кибердиверсий, при котором осуществляется блокирование компьютерной информации, являются атаки типа DDoS[6].

Компьютерные преступники осуществляют DDoS-атаки также и по мотиву мести за публичное раскрытие личностей преступников либо способов совершения компьютерных преступлений, а также для централизованного сбора денежных средств в целях финансирования долгосрочных таких атак.

Среди мотивов совершения преступления у кибертеррористов могут преобладать корыстные интересы; мотивы политической, идеологической, расовой, национальной или религиозной ненависти или вражды; мотивы мести за правомерные действия других лиц либо за осуществление лицом служебной деятельности или выполнением общественного долга; цели оправдания и поддержки терроризма. При осуществлении преступной деятельности в соучастии возможны различные сочетания вышеназванных мотивов.

Специализация *крэкеров* основана на обходе систем защиты прикладного программного обеспечения для предоставления возможности безвозмездного его использования неопределенному кругу лиц. Крэкерам обычно свойственен корыстный мотив совершения преступления в сочетании с так называемым «игровым мотивом» преступного поведения либо проявление любознательности.

Хакером может называться только лицо, обладающее профессиональными познаниями в компьютерной сфере (взлома систем, сетей, программ и др.). Лиц, пользующихся чужими наработками для взлома компьютерных систем и обычно малосведущих в механизме работы того или иного программного кода либо выдающие чужие наработки за свои собственные (это наихудшее с позиции приверженцев хакерской деятельности), в специальной литературе называют *скрипт-кидди*[7]. Им обычно свойственны корыстные побуждения (стремление к быстрой наживе), хотя и не исключается мотив личной неприязни (месть). В некоторых атипичных ситуациях скрипт-кидди могут причинять больший вред системам, в которую пытаются получить доступ. Иными словами, если хакеру доставляет особое удовольствие сам процесс неправомерного доступа к системе (деятельный аспект), желание решить сложную задачу, то для скрипт-кидди важным является сам факт неправомерного доступа с определенной целью. Скрипт-кидди можно назвать профессиональными преступниками с

6 От англ. аббревиатуры DDoS (distributed denial of service, т. е. распределенная атака типа «отказ в обслуживании»). Без наличия неправомерного доступа к большому количеству пользовательских компьютеров (компьютерных машин) компьютерный преступник не имеет возможности осуществлять атаки типа DDoS. В силу такой специфики деятельности в неправомерном пользовании преступников находятся распределенные компьютерные сети по всему миру, что увеличивает возможность скрытия следов преступления и личности. В практике имеются случаи, когда преступники, разочарованные прерыванием своей преступной деятельности службами безопасности, осуществляют в последующем атаки на такие ресурсы [См., например: Как мы не даем кардерам…, 2015, www].

7 От англ. script kiddie, что дословно означает «детский сценарий». На рост количества преступников скрипт-кидди значительное влияние оказывает распространение пошаговых инструкций (пособий) ко взломам. Ряды скрипт-кидди пополняют в основном лица, которые руководствуются сиюминутными потребностями, не располагая способностями и необходимым компетенциями.

большой долей условности. Поэтому им не свойственно скрывать следы своей преступной деятельности, проявлять необходимое усердие по сокрытию своей личности. По этой причине их неправомерные действия достаточно часто и легко обнаруживаемы.

Вирусмейкер – создатель вредоносной (т. е. предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации) компьютерной программы или информации. Ранее результатом такой деятельности рассматривалось создание компьютерных программ, уничтожающих информацию (например, компьютерных вирусов). В настоящее время создаются программные средства блокирующие, модифицирующие, копирующие компьютерную информацию (трояны, блокираторы). Одним из примеров использования программ-вымогателей является блокировка компьютеров Муниципального транспортного агентства Сан-Франциско (США) с требованием перечисления 73 тыс. долларов США за разблокировку компьютера [Krebs, 2016, www]. Иными словами, здесь наблюдается изменение мотивационной составляющей таких преступных деяний: мотив удовлетворения тщеславия сегодня все чаще вытесняется мотивом корыстной заинтересованности.

Заключение

Компьютерных преступников отличает умение четко формулировать возникающие проблемы. Обычно это свойственно лицам, обладающим хорошими знаниями языков программирования. Вместе с тем, убедительное логическое обоснование при выполнении задач в профессиональном плане, соседствует с хаосом в быту. Признается, что хакеры обладают эгоцентричным характером и крайне чувствительно воспринимают любое давление. В них немыслимым образом может сочетаться восторженный романтизм с самым гнусным цинизмом. Ведение преимущественно «ночного» образа жизни определяется возможностью исключить «отвлекающие факторы», наличием дешевого тарифа на доступ в сеть Интернет, занятостью в дневное время.

Большинство арестованных хакеров отмечают, что они некомфортно чувствуют себя в обществе и являются интровертами, отличаются фрустрацией в личных и общественных отношениях, отсутствием эмпатии и лояльности к обществу. Многим из них присуща в некоторой степени апатия [Chidambaram, 2012, www]. С другой стороны, в силу характера своей незаконной деятельности они представляются более целеустремленными и усидчивыми.

Таким образом, типизации компьютерных преступников не только может способствовать установлению подлинного смысла и содержание объективной и субъективной сторон составов преступлений, предусмотренных ст.ст. 272, 273 УК РФ. Существенное значение она имеет при реализации целей наказания (ст. 43 УК РФ) и разработке мер предупреждения преступности в сфере компьютерной информации.

Библиография

1. Шахназаров Г.Х., Батурин Ю.М. (ред.) Право и политика в компьютерном круге. Буржуазная демократия и «электронная диктатура». М.: Наука, 1987. 111 с.
2. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. 182 с.
3. Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказаний. Тамбов, 2003. 197 с.
4. Дремлюга Р.И. Интернет-преступность: дис. ... канд. юрид. наук. Владивосток, 2007. 248 с.
5. Дремлюга Р.И. Интернет-преступность. Владивосток: Изд-во Дальневост. ун-та, 2008. 240 с.
6. Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. … канд. юрид. наук. Иркутск, 2006. 203 с.
7. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. … канд. юрид. наук. М., 2003. 178 с.
8. Как мы не даем кардерам получать посылки, купленные на чужие кредитки // Блог компании Shopfans.ru. 2015. 29 мая. URL: https://geektimes.ru/company/shopfans/blog/250916/
9. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. … канд. юрид. наук. Пятигорск, 2010. 262 с.
10. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: дис. … канд. юрид. наук. Тамбов, 2007. 242 с.
11. Лацинская М. Group-IB представила отчет о хакерских атаках // Газета.Ру. 2016. 13 октября. URL: https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon_2016.shtml
12. Лейкина Н.С. Личность преступника и уголовная ответственность. Л.: ЛГУ, 1968. 128 с.
13. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук. М., 2006. 418 с.
14. Побегайло А.Э. Киберпреступность: лекция. М.: Академия Генеральной Прокуратуры Российской Федерации, 2013. 50 с.
15. Прокофьев В. ЦБ РФ опроверг информацию о краже хакерами 2 млрд. рублей с корсчетов // ТАСС информационное агентство. 2016. 3 декабря. URL: http://tass.ru/ekonomika/3837920
16. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. М., 2016. 232 с.
17. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой 24.05.1996: одобрен Советом Федерации 05.06.1996 // Собрание законодательства РФ. 1996. № 25. 17 июня. Ст. 2954.
18. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. 12 декабря. Ст. 7074.

19. Chidambaram V. The Profile of a Cyber Criminal // PC Advisor. 2012. 13 января. URL: http://www.pcadvisor.co.uk/feature/security/profile-of-cyber-criminal-3330068/
20. Krebs B. San Francisco Rail System Hacker Hacked // KrebonSecurity Internet Blog. 2016. 16 ноября. URL: https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/
21. Lowman S. Criminology of Computer crime. 2010. URL: https://www.lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf

The question of personality of computer criminals taking into account the nature and motivation of their criminal activities

Ramil' R. Gaifutdinov
Assistant,
Department of criminal law,
Kazan (Volga region) Federal University,
420008, 18 Kremlevskaya st., Kazan', Republic of Tatarstan, Russian Federation;
e-mail: gayfutdinov.r@yandex.ru

Abstract

The aim of this article is to study the personality of the individual categories of computer criminals taking into account the prevalence of existing titles. The author of this article talks about the rise of computer crime and produced damage. The bases of the proposed typology of the personality of a computer criminal are the specific features of the crime, contained in the relevant articles of the Criminal Code of the Russian Federation. The certain personal characteristics of the offender reveal in the method of implementation of the criminal activities of a computer criminal. According to the results of the study the author of this article draws to the new conclusions about the features of a social portrait of the personalities who commit cybercrime. Computer criminals are distinguished by the ability to formulate the problems. It is usually characteristic of individuals with a good knowledge of programming languages. It is recognized that hackers have a self-centered character and perceive any pressure extremely sensitively. They can combine the enthusiastic romanticism with the cynicism. Refined typology of computer criminals contributes to the establishment of the true meaning and content of crime definition of the corresponding penalty and developing measures of crime prevention in the sphere of computer information.

For citation

Gaifutdinov R.R. (2017) K voprosu o tipologii lichnosti komp'yuternykh prestupnikov s uchetom kharaktera i motivatsii ikh kriminal'noi deyatel'nosti [The question of personality of computer criminals taking into account the nature and motivation of their criminal activities]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 7 (4A), pp. 245-256.

Keywords

Computer criminality, computer crimes, personality of computer criminal, typology of personality of computer criminal

References

1. Chidambaram V. (2012) The Profile of a Cyber Criminal. *PC Advisor*, 13th Jan. Available at: http://www.pcadvisor.co.uk/feature/security/profile-of-cyber-criminal-3330068/ [Accessed 12/04/17].
2. Dremlyuga R.I. (2007) *Internet-prestupnost'. Dokt. Diss.* [Internet crime. Doct. Diss.]. Vladivostok.
3. Dremlyuga R.I. (2008) *Internet-prestupnost'* [Internet crime]. Vladivostok: Far East University.
4. Dvoretskii M.Yu. (2003) *Prestupleniya v sfere komp'yuternoi informatsii: ponyatie, sistema, problemy kvalifikatsii i nakazanii* [Crimes in the sphere of computer information: concept, system, problems of qualification and punishment]. Tambov.
5. Evdokimov K.N. (2006) *Ugolovno-pravovye i kriminologicheskie aspekty protivodeistviya nepravomernomu dostupu k komp'yuternoi informatsii. Dokt. Diss.* [Criminal law and criminological aspects of the prevention of illegal access to computer information. Doct. Diss.]. Irkutsk.
6. Kak my ne daem karderam poluchat' posylki, kuplennye na chuzhie kreditki [How we do not allow the carders to receive a parcel, bought on someone else's credit cards] (2015). *Blog kompanii Shopfans*.ru [Blog of company Shopfans.ru], 29th May. Available at: https://geektimes.ru/company/shopfans/blog/250916/ [Accessed 182/04/17].
7. Komarov A.A. (2010) Kriminologicheskie aspekty moshennichestva v global'noi seti Internet. Dokt. Diss. [Criminological aspects of fraud in the global Internet. Doct. Diss.]. Pyatigorsk.
8. Kopyryulin A.N. (2007) *Prestupleniya v sfere komp'yuternoi informatsii: ugolovno-pravovoi i kriminologicheskii aspekty. Doct. Diss.* [Crimes in the sphere of computer information: criminal law and criminological aspects. Doct. Diss.]. Tambov.
9. Krebs B. (2016) San Francisco Rail System Hacker Hacked. *Krebon Security Internet Blog*, 16th Nov. Available at: https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/ [Accessed 12/04/17].

10. Latsinskaya M. Group-IB predstavila otchet o khakerskikh atakakh [Group-IB presented the report about the hacker attack to the] (2016). *Gazeta.Ru*, 13th Oct. Available at: https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon_2016.shtml [Accessed 12/04/17].
11. Leikina N.S. (1968) *Lichnost' prestupnika i ugolovnaya otvetstvennost'* [Personality of offender and criminal liability]. L.: Leningrad State University.
12. Lopatina T.M. (2006) *Kriminologicheskie i ugolovno-pravovye osnovy protivodeistviya komp'yuternoi prestupnosti: Dokt. Diss.* [Criminological and criminal legal framework for combating computer crime. Doct. Diss.]. Moscow.
13. Lowman S. (2010) *Criminology of Computer crime*. Available at: https://www.lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf [Accessed 12/04/17].
14. Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii: ukaz Prezidenta RF ot 05.12.2016 № 646 [On approval of the Doctrine of information security of the Russian Federation: Decree of the President of the Russian Federation No. 646 of December 05, 2016] (2016). *Sobranie zakonodatel'stva RF (St. 7074)* [Collected legislation of the Russian Federation (Art. 7074)], 50, 12th Dec.
15. Pobegaĭlo A.E. (2013) *Kiberprestupnost'* [Cybercrime]. Moscow: Academy of The Prosecutor General of The Russian Federation].
16. Prokof'ev V. (2016) TsB RF oproverg informatsiyu o krazhe khakerami 2 mlrd. rublei s korschetov [Central Bank of the Russian Federation refuted information about the theft by hackers of 2 billion rubles from correspondent accounts]. *TASS informatsionnoe ag*entstvo [TASS News Agency], 3th Dec. Available at: http://tass.ru/ekonomika/3837920 [Accessed 15/04/17].
17. Prostoserdov M.A. (2016) *Ekonomicheskie prestupleniya, sovershaemye v kiberprostranstve, i mery protivodeistviya im. Dokt. Diss.* [Economic crimes committed in cyberspace and measures to counter them. Doct. Diss.]. Moscow.
18. Shakhnazarov G.Kh., Baturin Yu.M. (eds.) (1987) *Pravo i politika v komp'yuternom kruge. Burzhuaznaya demokratiya i "elektronnaya diktatura"* [Law and politics in the computer circle. Bourgeois democracy and "electronic dictatorship"]. Moscow: Nauka Publ.
19. Ugolovnyi kodeks Rossiiskoi Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi 24.05.1996: odobr. Sovetom Federatsii 05.06.1996 [Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996] (1996). *Sobranie zakonodatel'stva RF (St. 2954*) [Collected legislation of the Russian Federation (Art. 2954)], 25, 17th June.
20. Vekhov V.B. (1996) *Komp'yuternye prestupleniya: Sposoby sovershenia i raskrytiya* [Computer crimes: Ways of committing and disclosure]. Moscow: Pravo i Zakon Publ.
21. Zhmykhov A.A. (2003) *Komp'yuternaya prestupnost' za rubezhom i ee preduprezhdenie. Dokt. Diss.* [Computer crime abroad and its prevention. Doct. Diss.]. Moscow.