DOI: 10.17803/1994-1471.2022.138.5.149-158

М. В. Жижина*,
Д. В. Завьялова**

Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников)

Аннотация. Центральным элементом криминалистической характеристики преступлений в сфере компьютерной информации является личность преступника. В ее аспекте возможно изучение особенностей остальных элементов, установление их взаимосвязей и взаимозависимостей. Особенности соматических, психофизиологических и когнитивных процессов личности преступника, уровень его навыков в сфере информационных технологий, социальное окружение и профессиональная деятельность — все это предопределяет выбор способа, средств, обстановки совершения преступления и жертвы, а также механизм следообразования и локализацию следов. Вместе с тем вопросы, связанные с личностными особенностями современного киберпреступника, остаются открытыми из-за высокой волатильности, связанной со стремительным обновлением технических и технологических составляющих преступных деяний. Сегодняшние киберпреступники — это зачастую не угрюмые хакеры-одиночки, а хорошо организованная и структурированная преступная группа. В статье на основе анализа отечественных и зарубежных литературных источников, следственно-судебной практики предпринято исследование, направленное на восполнение данного пробела в доктрине.

* *Жижина Марина Владимировна*, доктор юридических наук, доцент, профессор кафедры криминалистики Московского государственного университета имени М. В. Ломоносова, главный научный сотрудник ФБУ РФЦСЭ при Минюсте России
Ленинские горы, д. 1, стр. 13 (4-й учебный корпус), г. Москва, Россия, 119991
mzhizhina@yandex.ru

** *Завьялова Дарья Владимировна*, старший преподаватель Департамента систем судопроизводства и уголовного права, заведующий криминалистической лабораторией НИУ «Высшая школа экономики»
Мясницкая ул., д. 20, г. Москва, Россия, 101000
dariazav@mail.ru

Ключевые слова: преступления в сфере компьютерной информации; личность; субъект; криминалистическая характеристика; особенности; элемент; российские и зарубежные источники; хакер; навыки; следственная практика; расследование.
Для цитирования: *Жижина М. В., Завьялова Д. В.* Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. — 2022. — Т. 17. — № 5. — С. 149–158. — DOI: 10.17803/1994-1471.2022.138.5.149-158.

Personality of the Subject of Crimes in the field of Electronically Stored Information as a System Forming Element of Forensic Characteristics (Based on Russian and Foreign Sources)

Marina V. Zhizhina, Dr. Sci. (Law), Associate Professor, Professor, Department of Criminalistics, Lomonosov Moscow State University; Chief Researcher, Russian Federal Centre of Forensic Science of the Ministry of Justice of the Russian Federation
Leninskie Gory, d.1, str. 13 (4th uchebnyy korpus), Moscow, Russia, 119991
mzhizhina@yandex.ru

Darya V. Zavyalova, Senior Lecturer, Department of Judicial Systems and Criminal Law, Head of the Forensic Laboratory, National Research University Higher School of Economics
ul. Myasnitskaya, d. 20, Moscow, Russia, 101000
dariazav@mail.ru

Abstract. The central element of the forensic characterization of crimes in the field of electronically stored information is the identity of the offender. In its aspect, it is possible to study the features of other elements, to establish their interrelations and interdependencies. Features of the somatic, psychophysiological and cognitive processes of the personality of the offender, the level of his skills in the field of information technology, the social environment and professional activity predetermine the choice of the method, means, the environment for the commission of the crime and the victim, as well as the mechanism of trace formation and localization of traces. At the same time, questions related to the personal characteristics of a modern cybercriminal remain open due to the high volatility associated with the rapid renewal of the technical and technological components of criminal acts. Today's cybercriminals are often not grim lone hackers, but a well-organized and structured criminal group. The paper studies and analyses domestic and foreign literary sources, investigative and judicial practice aiming at filling this gap.
Keywords: crimes in the field of electronically stored information; personality; subject; forensic characteristics; peculiarities; element; Russian and foreign sources; hacker; skills; investigative practice; investigation.
Cite as: Zhizhina MV, Zavyalova DV. Lichnost subekta prestupleniy v sfere kompyuternoy informatsii kak sistemoobrazuyushchiy element kriminalisticheskoy kharakteristiki (po materialam rossiyskikh i zarubezhnykh istochnikov) [Personality of the Subject of Crimes in the field of Electronically Stored Information as a System Forming Element of Forensic Characteristics (Based on Russian and Foreign Sources)]. *Aktual'nye problemy rossijskogo prava*. 2022;17(5):149-158. DOI: 10.17803/1994-1471.2022.138.5.149-158. (In Russ., abstract in Eng.).

Широко бытует обывательское представление, ассоциирующее киберпреступника с хакером — неким молодым нелюдимым гением информационных технологий, движимым корыстными или идеологическими мотивами. Более того, подобное мнение о хакере исключительно как о лице, совершившем преступление в сфере компьютерной информации или с использованием сети Интернет, и об основном источнике угроз

компьютерной безопасности имеет место и в доктрине[1].

Кроме того, в исследованиях, посвященных личностным особенностям субъекта киберпреступлений, авторы наделяют его высоким уровнем интеллекта, креативностью, находчивостью, нестандартным мышлением, скрытностью, часто — чувством собственного превосходства. Хакерам приписывают следующие типичные черты: необщительность, скромность, предпочитание виртуального мира живому общению, психологическая уязвимость, лабильность, высокое самомнение, исполнительность и добросовестность как работников, низкий уровень соблюдения трудовой дисциплины[2]. Не оспариваем большинство приведенных позиций, вместе с тем такой взгляд нам представляется несколько устаревшим.

На сегодняшний день бóльшая часть хакерского сообщества является законопослушными гражданами и выглядит совсем иначе. Многие из них осуществляют деятельность в целях защиты информационных систем и продвижения информационных технологий для большей доступности людям по всему миру[3].

Такой же искаженный образ сложился и у самого действия, определяемого глаголом «взломать» (от англ. hack — «взломать»). Предполагается, что «взлом» обязательно связан с преступной деятельностью, тогда как на самом деле это просто навык обращения с компьютерными системами, который так же, как и любой другой, может быть нацелен на решение совершенно разных задач (в том числе законных и правоохранительных) в зависимости от мотивации носителя этого навыка.

Обстоятельный анализ подходов к определению термина «хакер» в уголовно-правовых исследованиях был проведен А. И. Халиуллиным[4], и мы не видим смысла повторять его. Вместе с тем отметим, что считаем более корректным использование англоязычного термина «крэкер» (от англ. crack — «расколоть») для обозначения тех, кто «ломает» компьютерные системы со злым умыслом, используя свои знания и навыки в целях совершения преступных деяний, и отграничение их от хакеров — тех, кто исследует технологию, компьютерные системы, но не совершает преступлений[5].

Однако, как свидетельствуют мировые тенденции, термин «хакер» устойчиво применяется в современных уголовно-правовых исследованиях для обозначения профессиональных преступников в сфере информационных технологий, использующих «взлом» информационной системы как способ совершения преступления. При этом выделяются специфичные побудительные мотивы совершения преступлений, свойственные субкультуре хакеров (познавательный, игровой, хулиганский, политический и т.д.), исключающие либо подчеркивающие вторичность корысти[6].

---

1 *Маслакова Е. А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук. М., 2008. С. 4, 46 ; *Малышенко Д. Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. … канд. юрид. наук. М., 2002. С. 16.

2 *Евдокимов К. Н.* Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. 2011. № 1 ; *Маслакова Е. А.* Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. 2014. № 1 (31).

3 Компьютерные преступления : руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонстрох. М., 1999. С. 91 ; *Дубягина О. П.* Криминологическая характеристика норм, обычаев и средств коммуникации криминальной среды : автореф. дис. … канд. юрид. наук. М., 2008. С. 20.

4 *Халиуллин А. И.* Хакер как правонарушитель в современных уголовно-правовых исследованиях // Российская юстиция. 2019. № 12. С. 21–23.

5 *Лопатин В. Н.* Информационная безопасность России : дис. … д-ра юрид. наук. СПб., 2000. С. 326 ; *Степанов-Егиянц В. Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М. : Статут, 2016. С. 59–65.

6 *Копырюлин А. Н.* Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : дис. … канд. юрид. наук. Тамбов, 2007. С. 167.

В зарубежной литературе особенности и иерархии хакерского сообщества представлены достаточно широко. Так, хакеров в зависимости от мотивов их деятельности дифференцируют следующим образом:

— «белые шляпы» (white hat) — «этичные хакеры» — лица, чья работа заключается в поиске слабых сторон, ошибок, уязвимостей в компьютерных системах с целью их устранения, усиления защиты;
— «черные шляпы» (black hat) — взламывают системы из преступного интереса (чаще всего из корысти или престижа);
— «серые шляпы» (grey hat) — их мотивы могут меняться в зависимости от ситуации;
— «хактивисты» — хакеры, использующие свои навыки для продвижения политических и социальных идей.

По уровню навыков различают следующие группы:

— новички, или «зеленые шляпы» (noob, newbie, green hats), — лица, которые только начали учиться «взлому» и обладают минимальным уровнем навыка; они не имеют фактически никакого статуса в хакерском сообществе;
— скрипт-кидди (script kiddies) — молодые хакеры, которые не обладают необходимыми знаниями для создания собственных инструментов хакерских атак и используют готовые решения, получаемые из сети Интернет;
— хакеры (hacker, leet) — профессионалы, элита сообщества, люди с обширными знаниями, развитыми навыками и пониманием устройства компьютера, протекающих в нем процессов, программного обеспечения, создающие программные продукты, автоматизирующие атаки на компьютерные системы[7].

По доступу к цели атаки среди хакеров выделяют:

— «внутренних» (insider hackers) — это пользователи компьютерной системы или сети на законных основаниях, действующие с превышением своих полномочий;
— «внешних» (outsider hackers) — посторонние лица[8].

Вместе с тем вопросы, касающиеся установления характеристики современного киберпреступника, остаются открытыми в силу высокой волатильности, обусловленной стремительным обновлением технических и технологических составляющих преступных деяний. Так, на заре становления Интернета и развития информационных технологий преступления, связанные с несанкционированным доступом к информации, созданием, распространением и использованием вредоносных программ, могли совершать только хакеры — «черные шляпы», обладающие достаточным опытом, знаниями и имеющие корыстный интерес. За последние 20 лет киберпреступность превратилась в прибыльный бизнес с различными рынками и четким разделением труда. Программисты, специалисты в области компьютерного оборудования, маркетологи развили платформы, позволяющие обмениваться опытом, учить, продавать готовые программные и аппаратные продукты[9]. Сегодня они достаточно легко доступны, что позволяет, например, скрипт-кидди совершать полноценные компьютерные атаки даже при условии низко развитых навыков.

Данные тенденции являются общемировыми. Так, по данным МВД России, преступления в сфере компьютерной информации носят в большинстве случаев групповой характер, что обусловлено в том числе необходимостью разных «специализаций» преступников: в программировании, криптографии, технической

[7] *Holt T. J., Bossler A. M., Seigfried-Spellar K. C.* Cybercrime and Digital Forensics. Introduction. Second Edition. Abingdon, Oxon : Routledge, 2018. P. 102–103.

[8] *Maimon D., Lounderback E. R.* Cyber-Dependent Crimes: an Interdisciplinary Review // The Annual Review of Criminology. 2018. 12:37. P. 16.5.

[9] *Maimon D., Lounderback E. R.* Op. cit. P. 16.4 ; McAfee, CSIS Report: Economic Impact of Cybercrime — No slowing down. 2018.

поддержке и пр.[10] Весьма разнообразны и их мотивы, включающие корысть, престиж и продвижение по социальной лестнице в рамках профессионального сообщества, развлечение, идеологические взгляды, месть[11], демонстрацию навыков в качестве рекламы для потенциального работодателя и др.

В совершение преступлений в сфере компьютерных технологий вовлечен широкий круг лиц, среди которых встречаются «нелюдимые гении», «любопытствующие дилетанты», «корыстные прагматики», т.е. можно сказать, что психологические, соматические и мотивационные характеристики типичных преступников очень неоднородны и требуют дифференциации.

Отечественные и зарубежные ученые — криминалисты и криминологи, исследовавшие личностные особенности преступника по данной категории преступлений, выделяют следующие его характеристики[12]: примерно в 90 % случаев киберпреступником является мужчина, ранее не судимый (более 95 % от общего количества преступников), проживающий в городском населенном пункте, имеющий временную или постоянную регистрацию. Преобладающий возраст — от 16 до 35 лет, причем исследователи отмечают «омоложение»: так, 10 % киберпреступников в мире — это несовершеннолетние в возрасте от 14 до 15 лет, а 90 % хакерских атак совершается людьми в возрасте до 20 лет[13].

По данным, приведенным К. Н. Евдокимовым[14], уровень образованности преступников распределился примерно поровну между тремя группами: среднее образование имели примерно 30 %, среднее специальное образование — 32 %, высшее и неоконченное высшее — 37,3 %. Из них 13,3 % являлись студентами или учащимися образовательных организаций, 24,7 % относились к категории служащих, 31,3 % — специалисты в области IT-технологий (инженеры-программисты, сетевые администраторы и т.п.). Преобладающее большинство (более 60 %) в официальных семейных отношениях не состояло.

Следует также отметить, что 65 % компьютерных преступников совершили преступление неоднократно, т.е. при привлечении к уголовной ответственности им было вменено два и более эпизода совершения преступлений в сфере компьютерной информации.

Проведенный нами анализ статистических данных Судебного департамента при Верховном Суде РФ по составам, предусмотренным ст. 272–274.1 УК РФ за 2016–2020 гг.[15], подтверждает вышеприведенные соотношения. Вместе с тем заметим, что статистические выкладки не до конца отражают реальную картину в связи с высочайшей латентностью данной категории

---

[10] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. М., 2019. С. 121.

[11] *Maimon D., Lounderback E. R.* Op. cit. P. 16.5.

[12] IT-справочник следователя : монография / под ред. С. В. Зуева. М. : Юрлитинформ, 2019. С. 77–78 ; *Поляков В. В.*, *Людкова Н. В.* Характеристика личности киберпреступников // Теоретические и практические проблемы организации раскрытия и расследования преступлений : сборник материалов Всерос. науч.-практ. конференции, Хабаровск, 22 апреля 2016 г. Хабаровск : ФГКОУ ВО ДВЮИ, 2016. С. 90–93 ; *Holt T. J., Bossler A. M., Seigfried-Spellar K. C.* Op. cit. P. 75.

[13] *Глазатова С. В.*, *Бурцева Е. В.*, *Медведева С. В.* Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. 2021. № 2. С. 7–10.

[14] *Евдокимов К. Н.* Криминологический портрет личности преступника, совершающего преступления в сфере компьютерной информации // Актуальные вопросы юридических наук в современных условиях : сборник научных трудов по итогам международной научно-практической конференции, Санкт-Петербург, 11 января 2018 г. Н. Новгород, 2018. С. 50–52.

[15] URL: https://www.cdep.ru›index.php?id=79. См.: Отчет о демографических признаках осужденных за 2017–2010 гг. ; Отчет о характеристике преступления, его рецидива и повторности по числу осужденных по всем составам преступлений УК РФ за 2017–2010 гг. ; Отчет об осужденных, совершивших преступления в несовершеннолетнем возрасте за 2017–2020 гг.

преступлений. Это подтверждает и тот факт, что, по данным аналитиков, только в 10 % случаев к уголовной ответственности были привлечены лица за совершение преступных деяний в составе группы по предварительному сговору или организованной группы; 90 % совершали преступление в одиночку[16], т.е., как правило, «попадаются» именно неопытные одиночки, организованные преступные сообщества остаются вне поля зрения правоохранителей.

Таким образом, типичный субъект рассматриваемой нами категории преступлений — молодой, ранее не судимый, проживающий в городе, не состоящий в официальном браке мужчина, обладающий определенными техническими навыками владения IT-технологиями.

При этом уровень этих навыков может существенно разниться. Проведенный нами анализ отечественных и зарубежных литературных источников и судебно-следственной практики позволил разделить субъектов на три подгруппы:

1) лица с разным уровнем развития навыков в сфере информационных технологий, не ведущие систематической преступной деятельности;
2) без развитых навыков в сфере информационных технологий или со средним их уровнем, ведущие систематическую преступную деятельность, зачастую состоящие в преступных группировках;
3) с высоким уровнем навыков в сфере информационных технологий, ведущие систематическую преступную деятельность.

Субъекты первой группы — это ситуативные преступники. Их мотивами могут выступать месть, корысть, хулиганские побуждения, иногда стремление скрыть другое преступление. Такие преступники, как правило, ранее не совершали преступлений, не имеют связей с преступным сообществом, не состоят на учете в правоохранительных органах. Так, например, г-н М., находясь на своем рабочем месте, используя систему 1С Retail, к которой он имел доступ в силу своей должности для реализации его трудовых функций, из корыстной заинтересованности, с целью вывода денежных средств со счетов абонентских номеров, используя свое служебное положение, получил неправомерный доступ к охраняемой законом компьютерной информации, повлекший за собой ее модификацию (был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ)[17]. Более того, как показали результаты проведенного нами обобщения судебно-следственной практики, субъекты данной группы, более чем в 60 % случаев являясь сотрудниками или бывшими сотрудниками организаций, совершают соответствующие деяния с использованием своего служебного положения и легального программного обеспечения (далее — ПО), баз данных организации.

Значительная часть субъектов второй группы (в специальной литературе их называют скрипткидди) обладает средними или низкими навыками в области информационных технологий[18], они обычно малосведущи в механизме работы того или иного программного кода. Преобладающим мотивом их преступной деятельности является корысть, хотя в отдельных случаях возможны личная неприязнь, месть. Для подготовки информационных атак используют уже готовые технические решения.

Как отмечают зарубежные авторы, сложившиеся теневые киберрынки включают в себя следующие услуги: а) Crime-as-a-Service (CaaS) — продажа готовых инструментов (например, вредоносного ПО); б) Infrastructure-as-a-Service (IaaS) — продажа элементов инфраструктуры (например, оборудования); в) Research as a Service (RaaS) — сбор и продажа данных (например, номеров банковских карт)[19]. Эти

[16] *Евдокимов К. Н.* Криминологический портрет личности преступника, совершающего преступления в сфере компьютерной информации. С. 50–52.

[17] Приговор Новгородского районного суда (Новгородская область) от 18.09.2019 № 1-414/2019 по делу № 1-414/2019.

[18] *Holt T. J., Bossler A. M., Seigfried-Spellar K. C.* Op. cit. P. 68.

[19] *Maimon D., Lounderback E. R.* Op. cit. P. 16.4 ; McAfee, CSIS Report: Economic Impact of Cybercrime — No slowing down. 2018.

рынки выставляют на продажу оборудование, ПО, обучающие материалы, конфиденциальные данные (номера банковских карт, персональные данные и пр.), полное сопровождение процесса совершения преступления, техническую поддержку, схемы «гарантии качества», справочные и помощь. При этом потенциальные покупатели могут искать соответствующие товары как на просторах сети Dark web («даркнеб») (например, форум cracked.to, nulled.to), так и на вполне легальных интернет-площадках или через активно вытесняющий Telegram мессенджер Discord, гарантирующий анонимность. По данным исследователей, наибольшим спросом пользуются услуги, связанные с созданием и распространением вредоносного ПО (55 %), а также «взлом» почты, сайтов и удаленных серверов (17 %).

Кроме того, теневые киберрынки все более глобализируются, не разделяясь по региональному или языковому признаку: многие объявления из русскоязычного сегмента можно увидеть на английских или арабских форумах. Сегодня можно говорить о широкой «демократизации», доступности, в том числе ценовой, и интернационализации компьютерных преступлений[20]. Вместе с тем, несмотря на анонимность пользователей сети Dark web, проведение анализа криминального киберрынка — его «продуктов», соотношения спроса и предложения, продавцов и покупателей — является необходимой составляющей расследования преступлений в сфере компьютерной информации и их профилактики. Подобная информация может лечь в основу выдвижения версий о субъекте на первоначальном этапе.

Вышеприведенные тенденции актуальны и для российских реалий: по данным проведенного нами обобщения судебно-следственной практики, большая часть всех преступлений в сфере компьютерной информации (около 95 %) совершается с использованием уже готовых программных или аппаратных инструментов.

Кроме того, для скрипт-кидди из-за отсутствия должной квалификации не характерно скрывать следы своей преступной деятельности. По этой причине их неправомерные действия достаточно часто и легко обнаруживаемы, что подтверждается материалами судебной практики. Пример: научный сотрудник ФГУ «Российский федеральный ядерный центр — Всероссийский научно-исследовательский институт экспериментальной физики» вступил в сговор с двумя лицами, они использовали вычислительные мощности находящегося в организации компьютерного оборудования, возможности служебной локальной сети, предназначенной для обработки конфиденциальной информации, для вычисления (майнинга) криптовалюты с помощью скачанной из сети Интернет программы[21].

Представители третьей группы — хакеры-профи. Как отмечают исследователи, они разительно отличаются от других типов компьютерных преступников своими профессиональными знаниями и навыками, как правило, являются также профессионалами в области программирования. Применяемый ими инструментарий во многом определяется личными предпочтениями преступников: некоторые принципиально не используют какое-либо ПО (например, продукцию Microsoft), другие — только ПО, написанное на «любимом» языке программирования; кому-то присущи определенные способы или методы получения неправомерного доступа (например, атаки типа SQL, XSS-инъекций, и т.д.)[22]. Анализируя подобные предпочтения, можно установить индивидуальный «почерк» субъекта.

Как правило, хакеры-профи имеют узкую специализацию. Среди них можно выделить:

[20] McAfee, CSIS Report: Economic Impact of Cybercrime — No slowing down. 2018 ; Check Point Research Security Report 2019. Volume 01. Cyber Attack Trends Analysis: Key Insights to Gear Up for in 2019.

[21] Приговор Саровского городского суда (Нижегородская область) от 17.09.2019 № 1-149/2019 по делу № 1-149/2019.

[22] *Гайфутдинов Р. Р.* К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. 2017. Т. 7. № 4А. С. 245–256.

а) фрикеров (специализируются на получении неправомерного доступа к системам защиты охранных систем); б) кибертеррористов (их специализация — киберсаботаж путем блокирования компьютерной информации DDoS-атаками в отношении правительственных структур, специальных служб и организаций); в) крэкеров (специализируются на обходе систем защиты прикладного ПО для предоставления возможности безвозмездного его использования неопределенному кругу лиц); г) вирусмейкеров (создают вредоносные компьютерные программы или информацию). Существенно различается и мотивация преступной деятельности: при преобладании корыстного мотива у всех специализаций он может сочетаться: у крэкеров — с «игровым» мотивом и «любознательностью»; у кибертеррористов — с политической, идеологической, национальной или религиозной ненавистью или враждой, местью за осуществление лицом служебной деятельности или выполнение общественного долга; у вирусмейкеров — с удовлетворением тщеславия.

Представители данной подгруппы зачастую становятся «наемными работниками» для выполнения разовой узконаправленной задачи — разработки различных программных продуктов. При этом об истинной цели подобной работы они могут быть и не проинформированы.

Таким образом, рассмотренные нами материалы демонстрируют наличие корреляционных связей между личностью преступника, уровнем его навыков в сфере информационных технологий, с одной стороны, и иными обстоятельствами, подлежащими доказыванию, в первую очередь — способом, с другой. Это выражается в действиях по подготовке к совершению преступления, например при искании необходимых «продуктов» или соучастников-профи, непосредственно самом исполнении действий, посткриминальном поведении, что является составляющими способа совершения преступления[23].

БИБЛИОГРАФИЯ

1. *Гайфутдинов Р. Р.* К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. — 2017. — Т. 7. — № 4А. — С. 245–256.
2. *Глазатова С. В.*, *Бурцева Е. В.*, *Медведева С. В.* Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. — 2021. — № 2. — С. 7–10.
3. *Дубягина О. П.* Криминологическая характеристика норм, обычаев и средств коммуникации криминальной среды : автореф. дис. … канд. юрид. наук. — М., 2008. — 26 с.
4. *Евдокимов К. Н.* Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. — 2011. — № 1. — С. 86–90.
5. *Евдокимов К. Н.* Криминологический портрет личности преступника, совершающего преступления в сфере компьютерной информации // Актуальные вопросы юридических наук в современных условиях : сборник научных трудов по итогам международной научно-практической конференции, Санкт-Петербург, 11 января 2018 г. — Н. Новгород, 2018. — С. 50–52.
6. Компьютерные преступления : руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх ; пер. с англ. В. И. Воропаева и Г. Г. Трехалина. — М. : Мир, 1999. — 351 с.
7. *Копырюлин А. Н.* Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : дис. … канд. юрид. наук. — Тамбов, 2007. — 242 с.
8. *Малышенко Д. Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. … канд. юрид. наук. — М., 2002. — 166 с.

[23] *Новик В. В.* Способ совершения преступления. Уголовно-правовой и криминалистический аспекты. СПб., 2002. С. 32 ; *Лопатин В. Н.* Указ. соч.

9. *Маслакова Е. А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук. — М., 2008. — 198 с.
10. *Маслакова Е. А.* Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. — 2014. — № 1. — С. 114–121.
11. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2018. — 105 с.
12. *Новик В. В.* Способ совершения преступления. Уголовно-правовой и криминалистический аспекты. — СПб., 2002. — 92 с.
13. *Поляков В. В.*, *Людкова Н. В.* Характеристика личности киберпреступников // Теоретические и практические проблемы организации раскрытия и расследования преступлений : сборник материалов Всерос. науч.-практ. конференции, Хабаровск, 22 апреля 2016 г. — Хабаровск : ФГКОУ ВО ДВЮИ, 2016. — С. 90–93.
14. *Степанов-Егиянц В. Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. — М. : Статут, 2016. — 190 с.
15. *Халиуллин А. И.* Хакер как правонарушитель в современных уголовно-правовых исследованиях // Российская юстиция. — 2019. — № 12. — С. 21–23.
16. IT-справочник следователя : монография / под ред. С. В. Зуева. — М. : Юрлитинформ, 2019. — 232 с.
17. *Maimon D., Lounderback E. R*. Cyber-Dependent Crimes: an Interdisciplinary Review // The Annual Review of Criminology. — 2018. — 12:37. — P. 16.5.
18. *Holt T. J., Bossler A. M., Seigfried-Spellar K. C*. Cybercrime and Digital Forensics. Introduction. — Second Edition. — Abingdon, Oxon : Routledge, 2018. — P. 102–103.

Материал поступил в редакцию 20 августа 2021 г.

REFERENCES (TRANSLITERATION)

1. Gajfutdinov R. R. K voprosu o tipologii lichnosti kompyuternyh prestupnikov s uchetom haraktera i motivacii ih kriminalnoj deyatelnosti // Voprosy rossijskogo i mezhdunarodnogo prava. — 2017. — T. 7. — № 4A. — S. 245–256.
2. Glazatova S. V., Burceva E. V., Medvedeva S. V. Kiberprestupleniya, sovershaemye nesovershennoletnimi: problemy rassledovaniya // Rossijskij sledovatel. — 2021. — № 2. — S. 7–10.
3. Dubyagina O. P. Kriminologicheskaya harakteristika norm, obychaev i sredstv kommunikacii kriminalnoj sredy: avtoref. dis. … kand. yurid. nauk. — M., 2008. — 26 s.
4. Evdokimov K. N. Osobennosti lichnosti prestupnika, sovershayushchego nepravomernyj dostup k kompyuternoj informacii (na primere Irkutskoj oblasti) // Sibirskij yuridicheskij vestnik. — 2011. — № 1. — S. 86–90.
5. Evdokimov K. N. Kriminologicheskij portret lichnosti prestupnika, sovershayushchego prestupleniya v sfere kompyuternoj informacii // Aktualnye voprosy yuridicheskih nauk v sovremennyh usloviyah: sbornik nauchnyh trudov po itogam mezhdunarodnoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 11 yanvarya 2018 g. — N. Novgorod, 2018. — S. 50–52.
6. Kompyuternye prestupleniya: rukovodstvo po borbe s kompyuternymi prestupleniyami / D. Ajkov, K. Sejger, U. Fonstorh ; per. s angl. V. I. Voropaeva i G. G. Trekhalina. — M. : Mir, 1999. — 351 s.
7. Kopyryulin A. N. Prestupleniya v sfere kompyuternoj informacii: ugolovno-pravovoj i kriminologicheskij aspekty: dis. … kand. yurid. nauk. — Tambov, 2007. — 242 s.
8. Malyshenko D. G. Ugolovnaya otvetstvennost za nepravomernyj dostup k kompyuternoj informacii: dis. … kand. yurid. nauk. — M., 2002. — 166 s.

9. Maslakova E. A. Nezakonnyj oborot vredonosnyh kompyuternyh programm: ugolovno-pravovye i kriminologicheskie aspekty: dis. … kand. yurid. nauk. — M., 2008. — 198 s.
10. Maslakova E. A. Lica, sovershayushchie prestupleniya v sfere informacionnyh tekhnologij: kriminologicheskaya harakteristika // Politika i pravo. — 2014. — № 1. — S. 114–121.
11. Metodicheskie rekomendacii po rassledovaniyu prestuplenij v sfere kompyuternoj informacii: uchebnoe posobie / pod red. I. G. Chekunova. — M. : Moskovskij universitet MVD Rossii imeni V. Ya. Kikotya, 2018. — 105 s.
12. Novik V. V. Sposob sovershеniya prestupleniya. Ugolovno-pravovoj i kriminalisticheskij aspekty. — SPb., 2002. — 92 s.
13. Polyakov V. V., Lyudkova N. V. Harakteristika lichnosti kiberprestupnikov // Teoreticheskie i prakticheskie problemy organizacii raskrytiya i rassledovaniya prestuplenij: sbornik materialov Vseros. nauch.-prakt. konferencii, Habarovsk, 22 aprelya 2016 g. — Habarovsk: FGKOU VO DVYuI, 2016. — S. 90–93.
14. Stepanov-Egiyanc V. G. Otvetstvennost za prestupleniya protiv kompyuternoj informacii po ugolovnomu zakonodatelstvu Rossijskoj Federacii. — M. : Statut, 2016. — 190 s.
15. Haliullin A. I. Haker kak pravonarushitel v sovremennyh ugolovno-pravovyh issledovaniyah // Rossijskaya yusticiya. — 2019. — № 12. — S. 21–23.
16. IT-spravochnik sledovatelya: monografiya / pod red. S. V. Zueva. — M. : Yurlitinform, 2019. — 232 s.
17. Maimon D., Lounderback E. R. Cyber-Dependent Crimes: an Interdisciplinary Review // The Annual Review of Criminology. — 2018. — 12:37. — P. 16.5.
18. Holt T. J., Bossler A. M., Seigfried-Spellar K. C. Cybercrime and Digital Forensics. Introduction. — Second Edition. — Abingdon, Oxon: Routledge, 2018. — P. 102–103.