

Научная статья  
УДК 343.918:[347.7:004.77](470)

**Георгий Фаризович Шипулин**  
*Московский политехнический университет»,  
Москва, Россия, podumai\_nad@mail.ru*

## **КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ ЛИЧНОСТИ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ПРЕСТУПЛЕНИЯ В СФЕРЕ ЭКОНОМИКИ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ СЕТЕЙ**

*Аннотация.* В статье анализируются особенности портрета личности преступника, совершающего преступления в сфере экономики с использованием компьютерных сетей. Для исследования указанной тематики применяются такие методы, как анализ, синтез, сравнение и аналогия. Для анализа используется широко наработанный материал по портрету личности преступника в сфере экономики и по личности преступника в сфере компьютерной информации. Представляется актуальная информация о личности и отдельных чертах киберпреступника. В статье проводится подробный анализ групп указанного вида преступлений. Кроме того, проанализирована классификация по степени подготовки преступников и профилю их деятельности. Также рассмотрены характерные черты типизации преступников, предложенные учеными. Автор приводит особенности личности преступника, совершающего преступление в сфере экономики, а также с использованием компьютерных сетей; проводится аналогия с личностью преступника, совершающего преступление в сфере экономики с использованием компьютерных сетей. В работе представлена актуальная нормативная база, статистические показатели и научная литература. На основе синтеза и анализа данной информации делается вывод о ряде черт, характеризующих портрет личности преступника, совершающего преступление в сфере экономики с использованием компьютерных сетей.

*Ключевые слова:* киберпреступления, компьютерные сети, компьютерная информация, портрет личности преступника

*Для цитирования:* Шипулин Г. Ф. Криминологический портрет личности преступника, совершающего преступление в сфере экономики с использованием компьютерных сетей // Общество, право, государственность: ретроспектива и перспектива. 2023. № 3 (15). С. 66–71.

Original article

**Georgy F. Shipulin**  
*Moscow Polytechnic University, Moscow, Russia,  
podumai\_nad@mail.ru*

## **CRIMINOLOGICAL PORTRAIT OF THE IDENTITY OF A CRIMINAL COMMITTING CRIMES IN THE FIELD OF ECONOMICS USING COMPUTER NETWORKS**

*Abstract.* The article analyses the peculiarities of the personality profile of a criminal who commits crimes in the field of economics using computer networks. For research of the specified theme such methods as the analysis, synthesis, comparison and analogy are used. For the analysis we use extensively researched material on the profile of economic criminals and on the profile of criminals in the field of computer information. Up-to-date information on the personality of cybercriminals and their traits is presented. The article provides a detailed analysis of groups of the specified type of a crime. The study analyses the classification according to the degree of training of offenders and the profile of their activities. Characteristic features of typification of criminals proposed by scientists are also investigated. The peculiarities of personality of the offender, who commits a crime in the sphere of economics, as well as with the use of computer networks, are considered; an analogy with the personality of the offender, who commits a crime in the sphere of economics with the use of computer networks is drawn.

© Шипулин Г. Ф., 2023

The research uses the current regulatory framework, statistical indicators and scientific literature. Based on the synthesis and analysis of this information, a conclusion is made about a number of features that characterize the personality profile of an offender who commits economic crimes using computer networks.

*Keywords:* cyber crimes, computer networks, computer information, portrait of the criminal's personality

*For citation:* Shipulin G. F. Criminological portrait of the identity of a criminal committing crimes in the field of economics using computer Networks // Society, law, statehood: retrospective and perspective. 2023. No. 3 (15). P. 66–71.

За последнее время получило широкое распространение использование компьютерных технологий во многих сферах народного хозяйства. Этому способствуют развитие и освоение технологий в областях технических и компьютерных наук, что позволяет хранить и обрабатывать большие массивы компьютерной информации за короткий период времени, объединять разрозненные компьютерные системы в локальные вычислительные сети, а также в глобальную сеть Интернет, обеспечивая тем самым между устройствами взаимодействие, и многое другое. Данные технологии не только позволили повысить эффективность ряда сфер народного хозяйства и государственных структур [1, с. 189], но и создали перечень новых областей, сформировавших как новые сектора экономики, так и новые формы общественных отношений [2, с. 9]. Наряду с созданием полезных для социума общественных отношений новые технологии создали пласт возможностей для противоправных деяний, которым начали пользоваться правонарушители. Данные виды правонарушений сформировали специфический портрет личности преступника, который обуславливается вновь появившимися общественными отношениями, не существовавшими до широкого распространения компьютерных сетей.

В целях исследования личности преступника, совершающего правонарушения в сфере экономики с использованием компьютерных сетей, рассмотрим уже изученные личности преступников, совершавших правонарушения в сфере экономики, и личности преступников, совершавших киберпреступления. Таким образом, совершив анализ и синтез данной информации, можно сделать вывод о преобладающих личност-

ных качествах лица, совершающего преступления в сфере экономики с использованием компьютерных сетей.

Рассмотрим особенности личности киберпреступников. Киберпреступность – достаточно новое явление, которое свойственно для нестандартных типов личности, зачастую замкнутых и асоциальных, но при этом с высоким уровнем образования и технической подготовки [3, с. 184]. Киберпреступники зачастую покушаются на новые формы общественных отношений, которые сформировались посредством развития и распространения компьютерных сетей. К новым формам общественных отношений можно отнести так называемое «интернет-общение», осуществляемое посредством мессенджеров, социальных сетей и других средств интернет-коммуникаций. Особенностью данного типа общения является то, что знакомство и общение преимущественно осуществляются посредством компьютерных сетей, при этом личное или «живое» общение между собеседниками может вообще отсутствовать. Данный формат трансформирует структуру общения и семантику «активного пользователя интернета» [4, с. 21], чему способствует анонимность и дистанционность взаимодействия лиц. Также исследователи отмечают, что на формат общения также влияют трудности в эмоциональном плане и стремление выделиться вызывающим поведением [5, с. 279].

Эти факторы создают в психике человека вторую «виртуальную» личность и позволяют легче переступить различные социальные барьеры, что в результате влияет не только на личность рядового пользователя, но и на личность правонарушителей, которые без этих факторов, свойственных «интернет-общению», могли не пересекать границы закона.

Компьютерные преступления могут быть разной степени подготовленности, совершаться в одиночку или в составе группы. Наиболее многочисленны преступления, происходящие без прямого взаимодействия с потерпевшим либо же с минимальной коммуникацией без физического контакта. Это существенно отличает данный вид экономических преступлений от совершаемых без участия компьютерных и телекоммуникационных технологий. Осуществление преступлений зачастую требует от исполнителя обладания сложными техническими навыками в сфере компьютерных технологий, что возможно лишь при предрасположенности к данным наукам, а также при наличии профильного образования в соответствующих учебных заведениях или же самообразования. Преступления, осуществляемые подобными злоумышленниками, обычно длительны по времени подготовки и зачастую задействуют большое количество людей, каждый из которых занят своей областью в общей задаче. При этом ошибочно считать, что преступления совершаются исключительно высококвалифицированными техническими специалистами. Среди лиц, совершающих подобные преступления, большое количество дилетантов, которые не обладают высоким уровнем технических навыков [6, с. 258], а пользуются пошаговыми инструкциями, т. е. «мануалами», которые обычно покупаются или выдаются организаторами преступных схем [7, с. 68]. Действуя по этим инструкциям, злоумышленники могут совершать тяжкие и особо тяжкие преступления, быстро набирая опыт за счет массовости совершаемых преступлений. Таким образом, два вида преступлений формируют две большие группы личностей преступников: профессионалы, специализирующиеся на сложных преступлениях, и профессионалы, действующие по заранее подготовленным инструкциям.

Рассмотрим типизацию преступников, которую предлагают различные ученые. Наиболее частым является разделение преступников по мотивам, среди которых специалисты выделяют следующие: корыстные, хулиганские, политические, игровые, исследовательский интерес, потребность в самоутверждении, месть, а также мотивы, связанные с психическими отклонениями [8]. Кроме того, компьютерных преступников принято разделять, как было замечено нами ранее, по степени подготовки: высококвалифицированные, низкоквалифицированные. Профессиональных компьютерных преступников можно классифицировать по профилю их деятельности:

1. Специализирующиеся на получении несанкционированного доступа.
2. Специализирующиеся на написании вредоносного программного обеспечения.
3. Специализирующиеся на блокировании критической информации с целью получения выкупа (кибер-вымогатели).
4. Специализирующиеся на атаках типа «отказ в обслуживании», которые приводят к нарушению работоспособности инфраструктуры организации.
5. Специализирующиеся на взломах по политическим мотивам<sup>1</sup>.

Разделяют киберпреступников также на одиночек, хакерские группировки, объединенные для достижения поставленных целей, и АРТ-группировки, которые обладают значительными техническими и интеллектуальными ресурсами. Последние представляют наиболее серьезную угрозу на уровне государств<sup>2</sup>. Преступления, совершенные профессионалами, составляют самую малую долю среди раскрытых преступлений [6, с. 259]. Доля одиночек в совершении преступлений оценивается в 80 % [8].

Можно сделать вывод, что преступления, осуществляемые с использованием компьютерной информации, совершают-

<sup>1</sup> Анатомия хакерских группировок: кто и зачем взламывает цифровые системы. URL: <https://forklog.com/anatomy-hackerskih-grupirovok-kto-i-zachem-vzlamyvaet-tsifrovye-sistemy> (дата обращения: 30.10.2022).

<sup>2</sup> Защита от целевых атак и АПТ. URL: [https://www.anti-malware.ru/analytics/Technology\\_Analysis/Targeted-attacks-risk-and-protection#part2](https://www.anti-malware.ru/analytics/Technology_Analysis/Targeted-attacks-risk-and-protection#part2) (дата обращения: 30.10.2022).

ся принципиально разными социальными группами людей, преследующих разные мотивы и использующих разные средства достижения целей. Объединяет все эти деяния лишь компьютерная информация, которая может являться как средством совершения преступления, так и объектом преступления.

Рассмотрим типизацию личности преступников, совершающих преступления в сфере экономики. Данный раздел включает в себя широкий спектр преступлений. Из предмета настоящего исследования можно сразу отказаться от рассмотрения разбойных и иных преступлений, связанных с применением насилия. Также не будем рассматривать большинство преступлений, охваченных главами 22 и 23 Уголовного кодекса Российской Федерации, в сфере экономической деятельности и против интересов службы в коммерческой организации. Остановимся на типах личности преступников, занимающихся кражами, мошенничеством, налоговыми преступлениями и вымогательствами, т. е. теми видами преступлений, которые зачастую совершаются с использованием компьютерных сетей.

Среди данных видов преступлений в сфере экономики можно выделить две большие группы преступников, совершающих их [9, с. 169]. К первой относятся лица, совершающие спонтанное и импульсивное хищение, характеризующееся слабой подготовленностью и отсутствием продуманности последствий. Лица, совершающие подобные правонарушения, зачастую обладают низким уровнем образования, неразвитыми коммуникативными навыками и выраженной маргинализированностью. Вид подобных преступлений небольшой и средней тяжести составляет большую часть от общего количества совершенных преступлений. Так, например, три четверти всех преступлений в сфере экономики, совершенных путем обмана и злоупотребления доверием, являются преступлениями небольшой и средней тяжести [10, с. 126]. Ко второй группе относятся лица, специализирующиеся на крупных хищениях. Они характеризуются высоким уровнем образования, развитыми коммуникативными или узкопрофессиональ-

ными навыками, позволяющими понимать «уязвимые места» финансовых институтов [11, с. 59], а также продуманностью действий для избегания последствий (предварительная договоренность с адвокатом о последующей защите; подготовка и документирование обстоятельств, смягчающих возможный приговор; совершение правонарушения способом, исключающим возможность формирования состава особо тяжкого преступления и т. д.). Также данных лиц отличает постоянное совершенствование своих криминальных навыков.

Сравнивая информацию о типах личностей преступников, совершающих компьютерные и экономические преступления, можно прийти к следующим выводам касательно личности преступника, совершающего преступления в сфере экономики с использованием компьютерных сетей. Среди данного типа преступников имеется разделение на две подгруппы профессионалов, действующих преимущественно в составе группы лиц, и «любителей», для которых возможности компьютерных сетей стали лишь очередным источником «легких денег». Таким образом, в данную сферу зачастую попадает множество дилетантов, совершающих преступления в сфере экономики с использованием компьютерных сетей при помощи подготовленных кем-то инструкций и инструментов автоматизации. Компьютерная сеть не является каким-либо объектом, изучение которого представляет интерес. Противоположностью являются профессиональные хакерские группировки, специализирующиеся на таких экономических преступлениях, как хищение и вымогательство. Их отличает глубокое знание предмета, длительное время подготовки к совершению преступления, а также анонимизация выполняемых действий с целью неоставления улик для следствия. Подобный тип личности отличается высоким уровнем образования, высоким интеллектом и наличием организаторских способностей. Общим для типов личностей преступников, совершающих преступления в сфере экономики с использованием компьютерных сетей, является продуманность и осознан-

ность совершаемых действий, так как способы совершения данного вида преступлений подразумевают наличие предварительного этапа планирования и подготовки, что исключает спонтанность подобных действий. Так как данные правонарушения совершаются по корыстным соображениям, то типы личности преступников, их совершающих, не будут соответствовать типам личностей преступников, совершающих компьютерные преступления из хулиганских или идеологических побуждений. Следовательно, низка вероятность наличия у личности комплексов нереализованных амбиций и идеалистических взглядов, и, наоборот, высока вероятность наличия материалистических взглядов. Хотя в редких случаях деньги могут быть лишь средством для достижения конечной цели, но данные мотивы крайне редки и в большинстве случаев получение денег является высшей и конечной целью

лица, совершающего киберпреступления в сфере экономики.

Подводя итог, можно сделать вывод, что личность, совершающая преступления в сфере экономики с использованием компьютерных сетей, обладает чертами, свойственными как личностям, совершающим преступления в сфере экономики, так и личностям, совершающим преступления в сфере компьютерной информации. При этом мелкие и ситуативные преступления, совершаемые лицами, не имеющими глубоких знаний в области компьютерных технологий и совершающими преступления по инструкции, разработанной иным лицом, более похожи на преступления лиц, совершающих преступления в сфере экономики. Лица же, обладающие глубокими знаниями в технической сфере, имеют больше схожих черт с лицами, совершающими преступления в сфере компьютерной информации.

## СПИСОК ИСТОЧНИКОВ

1. Осокин Р. Б., Дикажев М. М. Электронный документооборот в правоохранительных органах: состояние и проблемы правовой регламентации // Вестник Московского университета МВД России. 2020. № 6. С. 188–196.
2. Трунцевский Ю. В., Ефремов А. А. Цифровая интеграция – путь в будущее // Международное публичное и частное право. 2018. № 1. С. 6–12.
3. Трунцевский Ю. В. Интеллектуальное пиратство: гражданско-правовые и уголовно-правовые меры противодействия. Москва : ИГ Юрист, 2002. 283 с.
4. Куликова А. В. Особенности интернет коммуникаций // Вестник Нижегородского Университета им. Н. И. Лобачевского. Серия Социальные науки. 2012. № 4. С. 19–24.
5. Усачева А. В. Психологические особенности интернет-коммуникации // Вестник Университета. 2014. № 1. С. 277–281.
6. Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников // Известия АлтГУ. Юридические науки. 2018. № 6. С. 256–259.
7. Есаян А. К., Трунцевский Ю. В. О понятии и признаках схем совершения финансовых преступлений // Юридический мир. 2008. № 2. С. 67–69.
8. Ищук Я. Г., Пинкевич Т. В., Смолянинов Е. С. Цифровая криминология : учебное пособие. М. : Академия управления МВД России, 2021. 244 с.
9. Трунцевский Ю. В. Российское уголовно-превентивное право: признаки отрасли // Российский криминологический взгляд. 2010. № 3. С. 165–173.
10. Осокин Р. Б., Немтинов Д. В. К вопросу о признаках преступлений в сфере экономической деятельности, совершаемых путем обмана и (или) злоупотребления доверием // Общество и право. 2016. № 2. С. 121–128.
11. Осокин Р. Б., Клещенко Ю. Г. Проблемы квалификации налогового мошенничества по субъективным признакам // Вестник ТГУ. 2008. № 6. С. 357–360.

## REFERENCES

1. Osokin R. B., Dikazhev M. M. Electronic document management in law enforcement agencies: the state and problems of legal regulation//Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. № 6. P. 188–196. (In Russ.)
2. Truntsevsky Yu. V., Efremov A. A. Digital integration – the way to the future // International public and private law. 2018. No. 1. P. 6–12. (In Russ.)
3. Truntsevsky Yu. V. Intellectual piracy: civil and criminal legal measures of counteraction. M. : IG Lawyer, 2002. 283 p. (In Russ.)
4. Kulikova A. V. Internet Communications//Bulletin of Nizhny Novgorod University named after N. I. Lobachevsky. Social Sciences Series. 2012. No. 4. P. 19–24. (In Russ.)
5. Usacheva A. V. Psychological features of Internet communication//Bulletin of the University. 2014. № 1. P. 277–281. (In Russ.)
6. Polyakov V. V., Popov L. A. Personality features of computer criminals // Izvestia AltSU. Legal sciences. 2018. № 6. P. 256–259. (In Russ.)
7. Yesayan A. K., Truntsevsky Yu. V. On the concept and signs of schemes for committing financial crimes // Legal world. 2008. No. 2. P. 67–69. (In Russ.)
8. Ishchuk Y. G., Pinkevich T. V., Smolyaninov E. S. Digital criminology : textbook. M. : Academy of Management of the Ministry of Internal Affairs of Russia, 2021. 244 p. (In Russ.)
9. Truntsevsky Yu. V. Russian criminal preventive law: signs of the branch // Russian criminological view. 2010. No. 3. P. 165–173. (In Russ.)
10. Osokin R. B., Nemtinov D. V. On the question of signs of crimes in the field of economic activity committed by deception and (or) abuse of trust // Society and law. 2016. No. 2. P. 121–128. (In Russ.)
11. Osokin R. B., Kleshchenko Yu. G. Problems of qualification of tax fraud on subjective grounds // Bulletin of TSU. 2008. No. 6. P. 357–360. (In Russ.)

Статья поступила в редакцию 04.05.2023; одобрена после рецензирования 18.05.2023; принята к публикации 15.09.2023.

The article was submitted 04.05.2023; approved after reviewing 18.05.2023; accepted for publication 15.09.2023.