УДК 343.9
ББК 67.51

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЧНОСТИ ЛИЦА, СОВЕРШАЮЩЕГО ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Е. О. Филиппова

Оренбургский государственный университет (Оренбург, Россия)

Исследование посвящено криминологической характеристике личности лица, совершающего преступления в сфере компьютерной информации. Рассматриваются типичные социопсихологические особенности, мотивационные факторы, уровень компетенций и доступность технической среды, а также влияние социокультурных и экономических условий на преступную активность в киберпространстве. На основе обобщения эмпирических и теоретических данных выявляются основополагающие черты, формирующие риск преступного поведения, обсуждаются проблема профилактики и направления уголовно-правового реагирования. Работа направлена на углубление понимания феномена цифровой преступности и повышение эффективности мер предупреждения и реабилитации.

Ключевые слова: киберпреступность, личность правонарушителя, компьютерная информация, мотивация, техническая компетентность, профилактика, цифровая девиация.

CRIMINOLOGICAL CHARACTERISTICS OF THE PERSONALITY OF A PERSON WHO COMMITS CRIMES IN THE FIELD OF COMPUTER INFORMATION

E. O. Filippova

Orenburg State University (Orenburg, Russia)

The study is devoted to the criminological characterization of the personality of a person who commits crimes in the field of computer information. Typical socio-psychological features, motivational factors, the level of competence and accessibility of the technical environment, as well as the influence of socio-cultural and economic conditions on criminal activity in cyberspace are considered. Based on the generalization of empirical and theoretical data, the fundamental features that form the risk of criminal behavior are identified, the problem of prevention and the direction of criminal law response are discussed. The work is aimed at deepening understanding of the phenomenon of digital crime and increasing the effectiveness of prevention and ϕrehabilitation measures.

Keywords: cybercrime, identity of the offender, computer information, motivation, technical competence, prevention, digital deviation.

Doi: https://doi.org/10.14258/ralj(2026)1.17

Актуальность криминологической характеристики личности лица, совершающего преступления в сфере компьютерной информации, обусловлена стремительным развитием информационных технологий и возрастающей цифровизацией всех сфер жизнедеятельности общества. Современный мир невозможно представить без сети Интернет, цифровых коммуникаций и электронных систем, что, к сожалению, создает новые возможности и для преступной деятельности. Киберпреступность перестала быть маргинальным явлением и трансформировалась в одну из наиболее серьезных угроз для экономической стабильности, национальной безопасности и личной неприкосновенности граждан.

Термин «компьютерная информация» является производным от общего понятия «информация» (от англ. «information» — разъяснение, осведомление, понимание) [1]. Это собирательное понятие охватывает множество аспектов, связанных с передачей, хранением и обработкой данных в цифровой форме. Компьютерная информация включает в себя как структурированные, так и неструктурированные данные, которые могут быть обработаны с помощью программного обеспечения и технологий. В современном мире она охватывает текстовые, звуковые, графические, видеоматериалы и любые другие формы данных, обрабатываемых и передаваемых через информационные системы и сети [2, с. 150].

Масштаб ущерба от компьютерных преступлений исчисляется миллиардами, а их последствия затрагивают как отдельные индивидуумы, так и крупные корпорации, государственные институты. При этом традиционные криминологические подходы, сформированные в условиях изучения «классической» преступности, часто оказываются неэффективными при анализе виртуального пространства. Анонимность, глобальный характер, отсутствие физической границы и высокая технологичность киберпреступлений требуют глубокого понимания специфики личности, мотивации и поведенческих паттернов лиц, вовлеченных в эту деятельность.

Без четкого представления о том, кто является типичным киберпреступником — его психологии, уровне технических навыков, социокультурных особенностях, способах вовлечения и формирования преступных групп — невозможно разработать действенные меры предупреждения, эффективные методы расследования и адекватные программы реабилитации. Изучение данной личности позволяет не только выявлять факторы риска, но и формировать целевые программы кибербезопасности, обучать население цифровой гигиене, а также совершенствовать правоприменительную практику. Постоянное обновление технических средств и методов преступной деятельности делает данную тему динамичной и требующей непрерывного научного осмысления для адекватного реагирования на вызовы современности.

Криминологическая характеристика личности лица, совершающего преступления в сфере компьютерной информации, опирается на комплексный анализ биографических, социально-экономических, психологических и технических факторов.

Анализируя исследования, посвященные личным характеристикам лиц, совершающих преступления в области компьютерной информации, можно отметить, что авторы соглашаются во мнении о высоком уровне интеллекта таких лиц, их нестандартном мышлении, находчивости и творческом подходе. Часто авторы отмечают скрытность и чувство собственного превосходства. К особенностям характера компьютерных преступников можно отнести: избегание общения, скрытность, уход в виртуальную среду, предпочтение виртуальным взаимодействиям, психологическая уязвимость, эмоциональная нестабильность, высокая самооценка, исполнительность и ответственность в рабочих процессах, недисциплинированность [3, с. 88].

Однако А. И. Халиуллин отмечает, что нынешние представители хакерского сообщества имеют совершенно иную стереотипную картину и, как правило, придерживаются законопослушного поведения, уделяя основное внимание обеспечению безопасности информационных систем и содействию в доступности информационных технологий для всех граждан [4, с. 22].

В. В. Поляков и Н. В. Людкова отмечают, что более 60% преступников, совершающих компьютерные преступления, совершили их неоднократно [5, с. 91].

Современное понимание киберпреступника формируется под влиянием трансформации информационного общества: широкая доступность Интернета, распространение мобильных устройств и облачных сервисов, усиление роли цифровых навыков в повседневной и профессиональной жизни создали новую экосистему, где преступное поведение может быть реализовано анонимно, дистанционно и с высокой эффективностью. В этой среде личность правонарушителя нередко отличается от традиционных моделей, присущих «уличной» преступности, что требует специализированного криминологического подхода.

Во-первых, необходимо выделить возрастной и гендерный профили. Значительная доля правонарушителей в сфере компьютерной информации относится к молодым возрастным группам — подросткам и молодым взрослым. Это объясняется сочетанием раннего и интенсивного освоения цифровых технологий, большей склонности к экспериментированию и поиску признания в онлайн-среде,

а также слабой осознанностью последствий. В то же время наблюдается и растущий процент вовлечения лиц старшего возраста, обладающих профессиональными навыками и доступом к информационным ресурсам. Гендерный состав варьируется в зависимости от типа правонарушений: технически сложные атаки и преступления, требующие длительной подготовки, чаще совершаются мужчинами, тогда как определенные виды мошенничества и социально-инженерных манипуляций могут демонстрировать более сбалансированное распределение по полу.

Во-вторых, важен образовательный и профессиональный уровень. Киберпреступления нередко совершаются лицами с высоким уровнем технической грамотности: программистами, системными администраторами, специалистами по информационной безопасности или самоучками, интенсивно изучавшими сети и криптографию. Однако наряду с «хакерами-специалистами» существуют и рекруты, использующие готовые инструменты — так называемые «скрипт-кидди», чья преступная активность обусловлена простотой применения автоматизированных средств и доступностью руководств в открытом доступе. Таким образом, уровень квалификации влияет на сложность и масштаб преступлений, но не является единственным фактором риска.

В-третьих, мотивация преступлений в данной сфере разнообразна и включает материальную выгоду, политический активизм, личную неприязнь или желание самоутверждения, а также исследовательский интерес и демонстрацию мастерства. Экономические мотивы остаются доминирующими в большинстве случаев: мошенничество, кража данных, вымогательство посредством программ-вымогателей направлены на получение финансовой выгоды. Политическая мотивация проявляется в деятельности хактивистов, целью которых является привлечение внимания к общественным проблемам или совершение диверсий против государственных и корпоративных инфраструктур. Социально-психологические мотивы, такие как жажда признания в сообществах, месть и склонность к рискованному поведению, также играют значительную роль, особенно среди молодежи.

В-четвертых, криминологический профиль включает психологические характеристики: высокий уровень технического интереса и креативности сочетаются с чертами, повышающими склонность к девиантному использованию знаний — низким уровнем эмпатии, потребностью в адреналине, склонностью к антисоциальным формам коммуникации и иногда нарциссическими чертами. Необходимо подчеркнуть, что не все технически грамотные лица обладают антисоциальными чертами; преступное поведение возникает на стыке индивидуальных предрасположенностей и внешних обстоятельств: доступности инструментов, безнаказанности и наличия рынков сбыта. Значимым фактором служит также воспринимаемая легитимность или нелегитимность существующих норм: если индивид считает, что правоприменительные механизмы несправедливы или неэффективны, это может снижать барьеры к совершению преступлений.

В-пятых, социокультурные и экономические условия оказывают существенное влияние. Высокая безработица среди IT-специалистов, неразвитость рынка легитимных возможностей для самореализации, коррумпированность институтов и экономические санкции могут способствовать росту мотивации к преступной деятельности. В некоторых сообществах существуют субкультуры, романтизирующие взлом и противостояние властям, что создает среду для обмена навыками и вербовки новичков. Онлайн-платформы и форумы функционируют как каналы коммуникации, обучения и торга инструментами атаки или украденной информацией, что облегчает организацию преступной деятельности и размывает традиционные барьеры солидарности.

В-шестых, структура преступного поведения в киберпространстве характеризуется гибкостью, сетевой организацией и частой междисциплинарной кооперацией. Преступления могут быть совершены индивидуально, но многие крупные операции требуют кооперации специалистов разных профилей: разработчиков, операторов, аналитиков и «мулов» для отмывания средств. Анонимность и распределенная архитектура коммуникаций (использование VPN, криптовалют, даркнета) обеспечивают относительно низкие трансакционные издержки и высокую устойчивость к правоохранительному вмешательству. Это приводит к появлению профессиональных киберпреступных групп, функционирующих на принципах рынка: специализация, разделение труда и конкуренция.

В-седьмых, рецидив и криминальный путь в этой сфере часто пересекаются с профессиональной траекторией: лица, прошедшие через судебное преследование, могут сохранять технические навыки

и при отсутствии эффективной социальной реабилитации возвращаться к преступной деятельности. Наличие условного наказания или краткосрочного лишения свободы без программ по переобучению и трудоустройству снижает шансы на десоциализацию. Напротив, доступ к легальной занятости, поддержка со стороны общественных организаций и возможность участия в легитимных инициативах по кибербезопасности могут перенаправить мотивации и навыки в конструктивное русло.

В-восьмых, проблемой современной криминологической характеристики является методологическая сложность получения надежных данных. Многое скрыто в даркнете, а участники преступлений тщательно маскируют свою личность. Исследователи опираются на судебную практику, материалы оперативных подразделений, интервью с осужденными и мониторинг онлайн-платформ, что создает выборочные сдвиги. При этом междисциплинарные исследования, объединяющие криминологию, психологию, социологию и информационные технологии, дают более полную картину и позволяют выделять типы правонарушителей, прогнозировать риски и разрабатывать таргетированные программы профилактики.

Проведенное исследование криминологической характеристики личности лица, совершающего преступления в сфере компьютерной информации, подтверждает многогранность и динамичность данного феномена. Отсутствие единого, универсального профиля киберпреступника является ключевым выводом. Вместо этого мы наблюдаем спектр личностных типов — от подростков-«скрипткидди» до высокопрофессиональных киберкриминальных группировок и даже лиц, действующих в интересах организованных преступных сообществ. Объединяющими чертами часто выступают высокая техническая осведомленность, интеллектуальная любознательность, а также способность к абстрактному мышлению и решению сложных логических задач. Мотивационные аспекты варьируются от поиска самоутверждения и жажды острых ощущений до стремления к материальному обогащению, идеологических убеждений и корпоративного шпионажа.

Анонимность и глобальный характер киберпространства значительно влияют на формирование личности преступника, снижая порог внутренних запретов и способствуя деперсонализации жертвы. Это также создает иллюзию неуязвимости, что позволяет им действовать более дерзко и масштабно. Важность междисциплинарного подхода, объединяющего криминологию, психологию, социологию и информационные технологии, становится очевидной для всестороннего понимания проблемы. Только такой комплексный анализ способен раскрыть сложные взаимосвязи между личностными качествами, социальным окружением и технологическими возможностями.

Практические выводы из данного исследования имеют критическое значение для правоохранительных органов, разработчиков политик и образовательных учреждений. Они подчеркивают необходимость специализированной подготовки кадров, развития международного сотрудничества, формирования эффективных программ профилактики, включая повышение цифровой грамотности населения и этического хакинга. В условиях постоянной эволюции технологий и методов киберпреступности непрерывное изучение и адаптация криминологических характеристик остаются фундаментальной задачей для построения безопасного цифрового будущего.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Большая российская энциклопедия. URL: https://bigenc.ru/c/informatsiia-50086f/

2. Соломатина А. Г., Пушкарев В. В. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере // Вестник экономической безопасности. 2024. № 5. С. 149–155.

3. Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. 2011. № 1. С. 86–90.

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

5. 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.