



УДК 343.93/.94
МРНТИ 10.81.51

А.Е. Сарбасов

*Алматынская академия Министерства внутренних дел Республики Казахстан имени М. Есбулатова,
г. Алматы, Республика Казахстан*

ЛИЧНОСТЬ ПРЕСТУПНИКА В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ

Аннотация. В условиях стремительной цифровизации общества киберпреступность занимает особое место среди современных форм преступности, отличаясь высокой латентностью, транснациональным характером и динамичным развитием. Настоящая статья посвящена исследованию личности киберпреступника с позиций криминологии и ориентирована на выявление ключевых социально-демографических, психологических и мотивационных характеристик нарушителей. В работе рассматриваются основные типы киберпреступников, включая кибермошенников, хактивистов, кибертеррористов и инсайдеров, чья деятельность влечет серьезные последствия для информационной безопасности государства, общества и частного сектора. Анализ статистических данных Республики Казахстан позволил выявить возрастные и профессиональные особенности правонарушителей, а также наметить тенденции их трансформации в условиях цифровой экономики. Особое внимание уделено роли инсайдеров и организованных кибергрупп, использующих как технические знания, так и социальную инженерию. Сделан вывод о необходимости адаптации существующих криминологических подходов и разработки эффективной типологии киберпреступников для повышения результативности противодействия угрозам в киберпространстве.

Ключевые слова: киберпреступность; личность преступника; высокие технологии; криминология; хакер; социальная инженерия; инсайдер; хактивизм.

А.Е. Сарбасов

*Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясы,
Алматы қ., Қазақстан Республикасы*

ЖОҒАРЫ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ ҚЫЛМЫСКЕР ТҰЛҒАСЫ: КРИМИНОЛОГИЯЛЫҚ АСПЕКТ

Аннотация. Қоғамның жедел цифрлануы жағдайында киберқылмыс заманауи қылмыстың ерекше түрі ретінде айқындалып отыр. Ол жоғары латенттілікпен, трансұлттық сипатымен және қарқынды дамуымен ерекшеленеді. Бұл мақала криминология тұрғысынан киберқылмыскердің тұлғасын зерттеуге арналған және құқық бұзушылардың негізгі әлеуметтік-демографиялық, психологиялық және мотивациялық сипаттамаларын айқындауға бағытталған. Жұмыста кибералаяқтар, хактивистер, кибертеррористер мен инсайдерлерді қоса алғандағы киберқылмыскерлердің негізгі түрлері қарастырылады. Қазақстан Республикасының статистикалық деректерін талдау құқық бұзушылардың жас ерекшеліктері мен кәсіби бейінін, сондай-ақ цифрлық экономика жағдайында олардың трансформациялану үрдістерін анықтауға мүмкіндік берді. Инсайдерлердің рөлі мен ұйымдасқан киберқылмыстық топтардың қызметіне ерекше назар аударылды. Киберқылмысқа қарсы іс-қимылдың тиімділігін арттыру үшін криминологиялық тәсілдерді бейімдеу және киберқылмыскерлердің тиімді типологиясын әзірлеу қажеттігі туралы қорытынды жасалды.

Түйінді сөздер: киберқылмыс; қылмыскер тұлғасы; жоғары технологиялар; криминология; хакер; әлеуметтік инженерия; инсайдер; хактивизм.



A.E. Sarbassov

*The Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Yesbulatov,
Almaty, the Republic of Kazakhstan*

THE PERSONALITY OF A CRIMINAL IN THE FIELD OF HIGH TECHNOLOGIES: CRIMINOLOGICAL ASPECT

Abstract. In the context of rapid digitalization, cybercrime has emerged as a distinct and complex form of modern criminality, characterized by high latency, transnational nature, and dynamic development. This article focuses on the study of the cybercriminal's personality from a criminological perspective, aiming to identify the key socio-demographic, psychological, and motivational characteristics of offenders. The paper examines the main types of cybercriminals, including cyber fraudsters, hacktivists, cyberterrorists, and insiders, whose activities pose serious threats to the information security of the state, society, and the private sector. An analysis of statistical data from the Republic of Kazakhstan revealed the age and professional profiles of offenders, as well as trends in their transformation within the digital economy. Special attention is paid to the role of insiders and organized cyber groups. The study concludes on the necessity of adapting criminological approaches and developing an effective typology of cybercriminals to strengthen counteraction in cyberspace.

Keywords: cybercrime; offender's personality; high technologies; criminology; hacker; social engineering; insider; hacktivism.

DOI: 10.52425/25187252_2025_38_143

Введение. Современное общество находится в эпохе цифровой трансформации, где информационные технологии проникают во все сферы человеческой деятельности. Однако параллельно с прогрессом возникает и новая форма преступности – киберпреступность, представляющая серьезную угрозу для экономической безопасности, частной жизни граждан и государственных интересов. В отличие от традиционных преступлений, киберпреступления совершаются в виртуальном пространстве, что придает им особые характеристики: транснациональный характер, высокую латентность и сложность раскрытия.

Изучение личности преступника в сфере высоких технологий занимает особое место в современной криминологической науке. Если классическая криминология преимущественно рассматривала социальные, экономические и психологические факторы формирования преступного поведения, то в цифровую эпоху возникает потребность в принципиально новых подходах. Как отмечают казахстанские исследователи, личность преступника в криминологии понимается как совокупность

свойств, формирующих индивидуальность и влияющих на совершение преступления [1]. Киберпреступник нередко действует анонимно, используя сложные технические средства, что значительно затрудняет его выявление и прогнозирование будущих действий.

Рост числа киберпреступлений сопровождается их качественной трансформацией: от разрозненных атак отдельных лиц до масштабных кампаний, организованных преступными группами и даже государственными структурами. В этих условиях понимание специфики личности киберпреступника становится неотъемлемым условием для разработки стратегий кибербезопасности, совершенствования законодательства и эффективной профилактики цифровой преступности.

Целью настоящей статьи являются исследование и анализ личности преступника в сфере высоких технологий в контексте криминологических подходов, с учетом социально-демографических и психологических характеристик, а также тенденций развития киберпреступности в отечественной и зарубежной практике.



Задачей статьи являются выявление ключевых особенностей личности киберпреступников, анализ существующих проблем их типологизации и разработка предложений по совершенствованию мер профилактики и противодействия киберпреступности.

Материалы и методы. В исследовании применялся комплексный подход, включающий криминологический анализ для выявления особенностей личности киберпреступников, сравнительно-правовой метод для сопоставления национального законодательства с международными актами (в частности, с Будапештской конвенцией), а также статистический анализ данных Комитета по правовой статистике Республики Казахстан (далее – РК) за 2023-2025 гг. Дополнительно изучались материалы судебной практики, что позволило определить типичные схемы преступной деятельности и трудности их квалификации. Для уточнения выводов использовались психологические исследования и контент-анализ научной литературы и специализированных изданий. Такой подход обеспечил комплексное понимание проблемы и формирование обоснованных выводов.

Эмпирическую базу исследования составили статистические данные Комитета по правовой статистике и специальным учетам Генеральной прокуратуры РК за 2023-2025 гг., материалы судебной практики и аналитические отчеты. Теоретическую основу сформировали труды отечественных и зарубежных ученых по криминологии и информационной безопасности, а также международные правовые акты в сфере противодействия киберпреступности.

Результаты, обсуждение. В академических кругах, профессиональной сфере и этических дискуссиях о кибербезопасности общепринято использование классификации на «белых», «серых» и «черных» хакеров, однако границы между этими категориями остаются предметом дискуссий и не имеют четких универсальных определений [2]. Как отмечает Лоуренс Сандерс, доктор фило-

софии, профессор управленческой науки и систем в Школе менеджмента UB, серые хакеры противостоят системе власти, черные хакеры мотивированы поиском острых ощущений, а белые хакеры – так называемые «хорошие парни» – часто проявляют нарциссические черты личности [3].

Трудно не согласиться с мнением авторов, которые классифицируют хакерское сообщество на четыре иерархические группы: 1) хакеры-мастера (guru hacker) – высший уровень профессионализма; 2) ситуативные хакеры (casual hacker) – обладающие ограниченным набором навыков; 3) хакеры в процессе обучения (learning hacker) и 4) хакеры-новички (novice hacker). Особого внимания заслуживает тот факт, что представители двух последних категорий, несмотря на стремление к системному пониманию архитектуры киберпространства, в действительности не владеют достаточными техническими компетенциями для осуществления модификаций его фундаментальных процессов и структурных элементов [4].

Согласно данным Комитета по правовой статистике и специальным учетам за период с 2023 по апрель 2025 гг., подавляющее количество привлеченных к уголовной ответственности за правонарушения в сфере цифровизации и связи имели возраст от 21 до 39 лет – 90%¹, т.е. средний возраст, что связано с высокой цифровой грамотностью и активным использованием технологий представителями этой возрастной группы.

Многие злоумышленники обладают глубокими знаниями в области программирования, сетевых технологий и информационной безопасности, как показывает исследование больше половины привлеченных имеют высшее образование в сфере IT специальностей (2025 (апрель) – 37/52, 2024 – 25/33, 2023 – 11/20)².

Повышение уровня «компьютерной грамотности» преступников увеличивает латентность преступлений данного вида.

Особую обеспокоенность вызывает тенденция роста числа указанных

¹ Отчет №1-М «О зарегистрированных правонарушениях» // Правовая статистика [Электронный ресурс] – Режим доступа: <https://qamqor.gov.kz/crimestat/statistics> (дата обращения: 03.10.2025).



преступлений, совершенных в составе группы лиц (2025 (апрель) – 4, 2024 – 6, 2023 – 3)⁵. В отличие от традиционной преступности, киберпреступления часто совершаются удаленно, что позволяет преступникам объединяться в международные сети, что усложняет их поимку.

Различные научные подходы к изучению личности киберпреступников позволяют выделить основные группы, как наиболее часто встречающиеся в практике:

1. Кибермошенники – занимаются фишингом, кардингом, обманом через социальные сети. Данный тип киберпреступников наиболее распространенный в нынешний период времени, и представляет серьезную угрозу. Их деятельность отличается массовостью, высокой латентностью и глобальным характером, что усложняет борьбу с этим видом преступлений. Также не все схемы требуют глубоких технических знаний (например, фишинг через поддельные сайты или соцсети). Доступность готовых инструментов в даркнете (скрипты, ботнеты, базы данных). Особенно выделяется тот факт, что кибермошенничество имеет высокую доходность при минимальных рисках, т.к. жертвы часто не обращаются в правоохранительные органы (особенно при небольших суммах) либо делают это только спустя определенное время. Анонимность криптовалют и обезличенных платежных систем усложняет поиск денежных потоков. Большинство атак основаны на социальной инженерии, а не на взломах, люди сами передают пароли или скачивают вирусы.

При этом немаловажным фактором остается поведение самих пользователей, которые зачастую становятся источником утечек, размещая чрезмерный объем личной информации в сети. Как справедливо отмечают исследователи, серьезной проблемой является несоответствие между отношением и поведением пользователей Интернета в вопросах конфиденциальности, усугубляемое отсутствием должной осторожности при защите персональных данных [5].

2. Хакеры-одиночки – категория киберпреступников, которые взламывают системы из интереса или для личной выгоды. В отличие от группировок, их деятельность часто мотивирована не только материальной выгодой, но и личными амбициями, идеологией или стремлением к самоутверждению. В качестве одного из примеров можно привести случай с молодым человеком 24 лет, который, не имея высшего образования, в целях личностного роста, используя технологии онлайн-платформы Rhadamanthys, создал компьютерную программу, с помощью которой можно нарушить работу компьютера и компьютерных программ, а также блокировать, модифицировать хранящуюся на компьютере информацию, а также завладеть ею. Данную программу он распространял среди других пользователей через мессенджер Telegram в сети Интернет².

При этом примечательно, что для совершения подобных деяний не требуется особая квалификация либо длительная и сложная подготовка, достаточно наличия технического выхода в Интернет, хорошего девайса, а также определенной мотивации и настойчивости.

3. Члены организованных кибергрупп – участвуют в масштабных атаках, таких как вымогательство либо промышленный шпионаж. В мировой практике известно множество организованных кибергрупп, например, «Anonymous», китайские «APT» и др. В отличие от хакеров-одиночек, они действуют системно, обладают значительными ресурсами и часто связаны с транснациональной преступностью.

На увеличение численности таких группировок оказывает влияние феномен появления небольших высокотехнологичных преступных групп, работающих на криминальных рынках, сильно зависящих от Интернета. Как правило, в таких группах меньшинство являются профессиональными преступниками, а основной контингент составляют работники IT-компаний, банков и т.п. С известной долей преувеличения такие группы можно обозначить как «ОПГ

² Приговор по делу № 1-217 от 06.08.2024 г. суда № 2 г. Костанай Костанайской области [Электронный ресурс] – Режим доступа: <https://office.sud.kz/form/courtActs/documentList.xhtml> (дата обращения: 25.09.2025).



преступников в свободное от работы время» [6]. Жертвами таких группировок могут быть отдельные граждане, компании, а также государственные учреждения целых стран.

Так, 6 февраля 2024 года на платформе GitHub неизвестными лицами был опубликован массив конфиденциальных материалов, предположительно относящихся к китайской компании iSoon (Anxun), являющейся подрядчиком Министерства общественной безопасности Китая (MPS) и ассоциируемой со структурой Chengdu 404 (APT41). Анализ представленных данных позволяет предполагать, что как минимум одна хакерская группировка в течение более чем двух лет обладала устойчивым несанкционированным доступом к отдельным элементам критической инфраструктуры казахстанских операторов связи³.

Подобные факты подтверждают важность международного взаимодействия и необходимость согласованных действий государств в борьбе с киберугрозами. В этой связи заслуживает особого внимания Будапештская конвенция о киберпреступности 2001 года, которая закрепила единые стандарты уголовно-правовой ответственности за незаконный доступ к компьютерным системам, вмешательство в данные, использование вредоносных программ. Помимо этого, Конвенция предусматривает процессуальные механизмы сохранения и изъятия электронных доказательств, перехвата трафика и международного обмена информацией, что позволяет государствам более эффективно расследовать киберпреступления, выходящие за рамки национальных юрисдикций⁴.

Данный факт не только вызывает тревогу, но и говорит о необходимости улучшать меры кибербезопасности.

4. Инсайдеры – сотрудники компаний, т.е. лица, имеющие легальный доступ к конфиденциальной информации (сотрудники, бывшие работники, подрядчики), которые используют свои привилегии в преступных

целях. В Казахстане, как и во многих других странах, инсайдерские угрозы представляют серьезную проблему для информационной безопасности.

Согласно данным, приводимым Ю.В. Трунцевским, максимальную угрозу создает инсайдерская деятельность сотрудников, связанных с обслуживанием корпоративных сетей организации и обеспечением ее информационной безопасности, поскольку они обладают наибольшими профессиональными знаниями и возможностями для содействия преступлениям [7].

Инсайдеры – тип угроз, от которого сложно защититься. Предсказать поведение недовольного системного администратора или менеджера по продажам, лишённого бонуса, достаточно сложно. Часто их действия направлены на кражу персональных данных или коммерческой информации с целью дальнейшей перепродажи либо саботажа, например, путем внедрения вредоносного кода.

В криминологической теории инсайдеров условно делят на три группы:

- умышленные – совершают преступление ради выгоды, мести, саботажа;
- неосторожные – нарушают правила в результате незнания или пренебрежения политиками безопасности;
- рекрутированные – подвергаются внешнему влиянию (шантаж, подкуп).

5. Участники хактивистской деятельности – особая категория субъектов киберпреступности, чьи действия мотивированы идеологическими и политическими убеждениями, а не корыстными интересами. Хактивизм – деятельность, осуществляемая с использованием информационных технологий и направленная на достижение идеологических, политических или социальных целей; в отдельных случаях может принимать противоправный характер. Термин «хактивизм» (от английского *hack* и *activism*) введен в научный оборот в 1990-х гг. Дж. Сэком. На мировой арене выделяются несколько хакерских групп, объединенных таким умыслом,

³ Китайская хакерская группировка контролировала критические объекты IT инфраструктуры Казахстана // Служба реагирования на компьютерные инциденты (CERT-Kazakhstan). – 20 февр. 2024 г. [Электронный ресурс] – Режим доступа: <https://cert.kz/news/chinese-hacker-group-controlled-critical-it-infrastructure-facilities-in-kazakhstan/> (дата обращения: 28.09.2025).

⁴ Budapest, 23.XI.2001 [Электронный ресурс] – Режим доступа: <https://rm.coe.int/1680081561> (дата обращения: 25.09.2025).



наиболее известные «Anonymous», «Killnet» и др.

Киберпреступники, особенно действующие в одиночку, обладают уникальным сочетанием высокого интеллекта и творческого мышления, что позволяет им находить нестандартные способы обхода даже самых сложных систем защиты. Их деятельность часто мотивирована не столько материальной выгодой, сколько внутренней потребностью в интеллектуальном вызове – многие воспринимают процесс взлома как своеобразную игру или соревнование, где главной наградой становится сам факт преодоления защитных механизмов. Эта специфическая психология сочетает в себе аналитический склад ума, способность быстро обрабатывать большие объемы информации и нестандартный подход к решению задач, что делает таких преступников особенно опасными. При этом склонность к риску и азартное отношение к своей противоправной деятельности только усиливают потенциальную угрозу, поскольку заставляют постоянно совершенствовать методы атак и искать новые уязвимости в защитных системах. В отличие от обычных преступников, они часто действуют не по шаблону, а создают уникальные схемы взлома, что существенно осложняет работу правоохранительных органов по их выявлению и задержанию.

На самом деле у хакеров значительно выше потребность в познании и склонность к риску, чем у широкой публики. Они склонны предпочитать рациональный стиль мышления интуитивному и демонстрируют особенно

высокую уверенность в своей способности принимать оптимальные решения в процессе рационального обдумывания. Предпочитают сложные задачи простым и получают больше удовольствия от решения задач, требующих напряженного мышления, чем среднестатистический человек [8].

Закключение. Проведенное исследование подтвердило, что киберпреступность представляет собой новую форму преступной деятельности, отличающуюся от традиционной высокой латентностью, транснациональным характером и повышенной технической сложностью. Криминологическая характеристика личности киберпреступника выявила преобладание молодых, технически подкованных лиц, зачастую с высшим IT-образованием.

Типология киберпреступников позволила глубже понять их мотивацию и поведенческие особенности, что важно для разработки мер профилактики и противодействия. Особое внимание следует уделить роли социальной инженерии, анонимных платежных систем и доступности вредоносных инструментов, что значительно упрощает совершение преступлений даже лицами с невысоким уровнем специальной подготовки.

Полученные результаты уточняют научные представления о субъекте преступления в цифровой среде и обосновывают необходимость междисциплинарного подхода к изучению киберугроз. В перспективе важным направлением остается разработка поведенческих моделей киберпреступников и совершенствование нормативно-правового регулирования в сфере кибербезопасности.

Список использованной литературы:

1. Омарова, А.Б. К понятию личности преступника преступлений в сфере компьютерной информации / А.Б. Омарова, Ш.Б. Маликова // Вестник КазНУ. Серия: юридическая. – 2016. – № 3 (79). – С. 293-297.
2. Canudo, M. Differentiating Hackers and Hacker Types: the Role of Self-Control, Personality and Motivations / M. Canudo, et al. – 2025. – 64 p.
3. Manne, K. Inside the mind of a hacker. – 2020 [Электронный ресурс] – Режим доступа: <https://www.buffalo.edu/news/news-releases.host.html/content/shared/mgt/news/inside-mind-hacker.detail.html> (дата обращения: 30.09.2025).
4. Bartko, R. Hackers in duty of cyberterrorism / R. Bartko, R. Kelemen // Journal of Infrastructure, Policy and Development. – 2025. – № 9 (2). – 10979.
5. Ерболатов, Е.Е. Баланс цифровизации и защиты персональных данных: казахстанский кейс / Е.Е. Ерболатов, С.Қ. Жетпісов // Құқық қорғау органдары академиясының Жаршысы. –



2024. – № 34 (4). – С. 26-34.

6. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский. – М.: Норма ИНФРА, 2019. – 352 с.

7. Трунцевский, Ю.В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения / Ю.В. Трунцевский // Российский следователь. – 2014. – № 21. – С. 19-22.

8. Bachmann, M. The Risk Propensity Computer Hackers and Rationality / M. Bachmann // International Journal of Cyber Criminology. – 2010. – Vol. 4. Issue 1. – Pp. 643-656.

References:

1. Omarova, A.B. K ponjatiju lichnosti prestupnika prestuplenij v sfere komp'yuternoj informacii / A.B. Omarova, Sh.B. Malikova // Vestnik KazNU. Serija: juridicheskaja – 2016. – № 3 (79). – S. 293-297.

2. Canudo, M. Differentiating Hackers and Hacker Types: the Role of Self-Control, Personality and Motivations / M. Canudo, et al. – 2025. – 64 p.

3. Manne, K. Inside the mind of a hacker. – 2020 [Jelektronnyj resurs] – Rezhim dostupa: <https://www.buffalo.edu/news/news-releases.host.html/content/shared/mgt/news/inside-mind-hacker.detail.html> (data obrashhenija: 30.09.2025).

4. Bartko, R. Hackers in duty of cyberterrorism / R. Bartko, R. Kelemen // Journal of Infrastructure, Policy and Development. – 2025. – № 9 (2). – 10979.

5. Erbolatov, E.E. Balans cifrovizacii i zashhity personal'nyh dannyh: kazhastanskij kejs / E.E. Erbolatov, S.Қ. Zhetpisov // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 34 (4). – С. 26-34.

6. Ovchinskij, V.S. Kriminologija cifrovogo mira: uchebnik dlja magistratury / V.S. Ovchinskij. – М.: Norma INFRA, 2019. – 352 s.

7. Truncevskij, Ju.V. Kiberprestuplenija v korporativnoj srede: riski, ocenka i mery preduprezhdenija / Ju.V. Truncevskij // Rossijskij sledovatel'. – 2014. – № 21. – S. 19-22.

8. Bachmann, M. The Risk Propensity Computer Hackers and Rationality / M. Bachmann // International Journal of Cyber Criminology. – 2010. – Vol. 4. Issue 1. – Pp. 643-656.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Алихан Ержанұлы Сарбасов – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының докторанты, ұлттық қауіпсіздік және әскері іс магистрі, e-mail: alihosarbas@gmail.com.

Сарбасов Алихан Ержанович – докторант Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, магистр национальной безопасности и военного дела, e-mail: alihosarbas@gmail.com.

Sarbassov Alikhan Erzhanovich – Doctoral Student of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Yesbulatov, Master of National Security and Military Case, e-mail: alihosarbas@gmail.com.