Копьёва Ксения Алексеевна
Студентка
Научный руководитель
Титов Сергей Николаевич
канд. юрид. наук, доцент
ФГБОУ ВО «Ульяновский государственный
педагогический университет им. И.Н. Ульянова»
г. Ульяновск, Ульяновская область

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЧНОСТИ КИБЕРМОШЕННИКА: ТИПОЛОГИЯ И ПОВЕДЕНЧЕСКИЕ ПАТТЕРНЫ

Аннотация: *в статье рассматривается криминологическая характеристика личности кибермошенника, проводится типологизация таких преступников и анализируется их поведенческие паттерны. Актуальность исследования обусловлена ростом числа киберпреступлений и необходимостью разработки эффективных мер противодействия кибермошенничеству [3]. В работе использованы методы анализа научной литературы, обобщения эмпирических данных, сравнительного и статистического анализа. Результаты исследования позволяют выделить ключевые черты личности кибермошенников, классифицировать их по различным критериям и описать типичные модели поведения. Полученные данные могут быть использованы для совершенствования профилактических мер и повышения эффективности расследования киберпреступлений.*

Ключевые слова: *кибермошенничество, криминология, личность преступника, типология, поведенческие паттерны, киберпреступность, профилактика преступлений.*

В условиях цифровой трансформации общества кибермошенничество становится одной из наиболее актуальных угроз безопасности. По данным МВД РФ, в последние годы наблюдается устойчивый рост числа преступлений, совершаемых с использованием информационно-коммуникационных технологий [3]. Это

обуславливает необходимость глубокого изучения личности кибермошенника с криминологической точки зрения.

Цель данной статьи – провести комплексный анализ криминологических характеристик личности кибермошенника, разработать типологию таких преступников и выявить их ключевые поведенческие паттерны. Для достижения этой цели поставлены следующие задачи:

– проанализировать научные подходы к изучению личности кибермошенника [1, с. 498];

– выделить основные черты личности кибермошенника;

– разработать типологию кибермошенников;

– описать типичные поведенческие паттерны;

– предложить направления профилактики кибермошенничества на основе полученных данных.

Личность кибермошенника имеет ряд специфических черт, отличающих её от личности традиционного преступника. К основным характеристикам можно отнести:

1) высокий уровень технической грамотности. Кибермошенники обладают знаниями в области информационных технологий, программирования, сетевых протоколов и методов социальной инженерии [2, с. 184];

2) возрастные особенности. Большинство кибермошенников – молодые люди в возрасте от 18 до 35 лет, активно использующие цифровые технологии [3];

3) мотивационная сфера. Основными мотивами совершения кибермошенничества являются корысть, стремление к быстрому обогащению, а также в отдельных случаях – желание самоутвердиться за счёт демонстрации своих технических навыков [4, с. 256];

4) психологические особенности. Для кибермошенников характерны:

– склонность к риску;

– высокий уровень самоконтроля;

– развитые коммуникативные навыки (особенно в онлайн-среде);

– способность к манипулированию;

– низкий уровень эмпатии по отношению к жертвам [1, с. 498];

5) социальный статус. Часто кибермошенники имеют высшее или незаконченное высшее образование, работают в IT-сфере или смежных областях либо обучаются по соответствующим специальностям [2, с. 184].

На основе анализа эмпирических данных можно выделить следующие типы кибермошенников.

1. Новички. Они характеризуются низким уровнем технических навыков, действуют по готовым инструкциям, часто вовлечены в преступную деятельность через интернет-сообщества. Совершают такие преступления как фишинговые рассылки, простые схемы обмана в соцсетях.

2. Профессионалы. Характеризуются высоким уровнем технических знаний, разрабатывают собственные инструменты для совершения преступлений, координируют группы исполнителей. Совершают такие преступления как создание вредоносного ПО, масштабные фишинговые компании, взлом банковских систем.

3. Хактивисты. Их мотивация носит идеологический характер, стремятся привлечь внимание к какой-либо проблеме. Совершают такие преступления как DDoS-атаки, взлом сайтов с публикацией компроматов.

4. Инсайдеры. Они имеют доступ к конфиденциальной информации в организациях, используют его в корыстных целях. Совершают такие преступления как кража корпоративных данных, продажа коммерческой тайны.

5. Организованные группы. Они действуют в составе структурированных преступных сообществ, распределяют роли между участниками. Совершают такие преступления как многоэтапные схемы мошенничества с участием подставных лиц, отмывание денег.

Анализ поведенческих паттернов позволяет выделить следующие типичные модели действий кибермошенников [5].

1. Подготовка:

– сбор информации о потенциальных жертвах;

– выбор инструментов и методов атаки;

– создание инфраструктуры (фейковые сайты, почтовые ящики и т. д.).

2. Реализация:

– установление контакта с жертвой (через электронную почту, соцсети, мессенджеры);

– применение методов социальной инженерии (фишинг);

– получение доступа к учётным записям, банковским счетами т. п.

3. Сокрытие следов:

– использование анонимизирующих технологий;

– маскировка IP-адресов;

– удаление логов и других цифровых следов.

4. Легализация доходов:

– перевод средств через цепочки подставных счетов;

– конвертация в криптовалюты;

– покупка ликвидных активов.

На основе проведённого анализа можно предложить следующие направления профилактики кибермошенничества [6, с. 314]:

– повышение цифровой грамотности населения, обучение методам распознавания мошеннических схем;

– совершенствование законодательной базы в сфере кибербезопасности;

– развитие международного сотрудничества в борьбе с киберпреступностью;

– внедрение технических решений для выявления и блокировки мошеннических ресурсов;

– проведение профилактических мероприятий в образовательных учреждениях и на предприятиях.

Криминологический анализ личности кибермошенника позволяет выделить ряд ключевых характеристик, отличающих таких преступников от других категорий правонарушителей. Разработанная типология и описание поведенческих паттернов дают возможность более эффективно прогнозировать и предотвращать

кибермошенничество. Дальнейшие исследования в этой области должны быть направлены на изучение новых форм киберпреступности и адаптацию профилактических мер к изменяющимся условиям цифровой среды.

Список литературы

1. Бабаев М.М. Криминология: учебник для вузов / М.М. Бабаев, В.Е. Квашис. – М.: Юрайт, 2021. – 498 с.

2. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов. – М.: Право и закон, 2019. – 184 с.

3. МВД РФ. Статистика киберпреступлений за 2023 год. – URL: https://vk.com/away.php?to=https%3A%2F%2Fxn--b1aew.xn--p1ai&utf=1 (дата обращения: 23.04.2026).

4. Романовский Г.Б. Правовое регулирование киберпространства: монография / Г.Б. Романовский. – СПб.: Юридический центр Пресс, 2020. – 256 с.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149ФЗ ред. от 29 декабря 2025 года №568-ФЗ, вступают в силу с 1 сентября 2026 года. – URL: https://www.consultant.ru/document/cons_doc_LAW_103797/1febfbad05f7b09a520e8dc27ad681e7bcaf085f/ (дата обращения: 23.04.2026).

6. Ястребов О.А. Информационное право: учебник и практикум для академического бакалавриата / О.А. Ястребов. – М.: Юрайт, 2022. – 314 с.