

*Тхаитлов Тамерлан Бесланович,
магистрант 1 курса, 1 группы,
институт права экономики и финансов
Кабардино-Балкарский государственный университет
имени Х.М. Бербекова,
Нальчик, Россия*

**КИБЕРБЕЗОПАСНОСТЬ В КАБАРДИНО-БАЛКАРИИ: ВЫЗОВЫ
ЦИФРОВОЙ ЭПОХИ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ**

***Аннотация:** В условиях глобальной цифровизации киберугрозы приобрели характер системного вызова для национальной безопасности. Данная статья посвящена анализу регионального ландшафта киберпреступности в Кабардино-Балкарской Республике (КБР) и комплексной стратегии, реализуемой Министерством внутренних дел по её противодействию. Рассматриваются основные категории угроз – от массовых атак на граждан с использованием методов социальной инженерии до целевых действий против критической информационной инфраструктуры. Особое внимание уделяется эволюции правоохранительной деятельности, включающей интеграцию технологий искусственного интеллекта, масштабную профилактическую работу, развитие кадрового потенциала и межведомственную координацию. Делается вывод о формировании в КБР многоуровневой модели кибербезопасности, основанной на синтезе технологического превосходства, человеческого капитала и правового регулирования.*

Ключевые слова: кибербезопасность, киберпреступность, МВД по КБР, искусственный интеллект, социальная инженерия, критическая информационная инфраструктура, профилактика.

*Tkhaitlov Tamerlan Beslanovich,
1st year master's student, 1st group,
Institute of Law, Economics, and Finance
Kabardino-Balkarian State University named after Kh.M. Berbekov,
Nalchik, Russia*

CYBERSECURITY IN KABARDINO-BALKARIA: CHALLENGES OF THE DIGITAL ERA AND COUNTERMEASURES STRATEGIES OF THE MINISTRY OF INTERNAL AFFAIRS

***Annotation:** In the context of global digitalization, cyber threats have become a systemic challenge to national security. This article focuses on analyzing the regional landscape of cybercrime in the Kabardino-Balkarian Republic (KBR) and the comprehensive strategy implemented by the Ministry of Internal Affairs to combat it. It examines the main categories of threats, ranging from mass attacks on citizens using social engineering techniques to targeted actions against critical information infrastructure. The article also highlights the evolution of law enforcement efforts, including the integration of artificial intelligence technologies, extensive preventive measures, personnel development, and interagency coordination. It is concluded that the KBR has formed a multi-level cybersecurity model based on the synthesis of technological superiority, human capital, and legal regulation.*

***Keywords:** cybersecurity, cybercrime, Ministry of Internal Affairs of the KBR, artificial intelligence.*

Цифровая трансформация общества привела к параллельной эволюции угроз, перенеся традиционные формы мошенничества и посягательств в киберпространство. Кабардино-Балкарская Республика, являясь неотъемлемой частью единого информационного поля России, сталкивается со всем спектром современных киберугроз, адаптированных к местной специфике. Для правоохранительных органов это означает необходимость фундаментальной трансформации методов работы: от физического задержания преступника к цифровому расследованию, от реагирования на совершённое преступление к его прогнозированию и упреждению. Роль МВД по КБР в этих условиях перестала быть исключительно карательной; ведомство становится архитектором региональной системы кибербезопасности, выстраивая оборону на стыке технологий, права и работы с гражданским обществом. Угрозы информационной безопасности в республике носят многоуровневый характер, отражая общероссийские тренды и создавая уникальные вызовы для местных правоохранителей. Наиболее массовой и ощутимой для населения остается волна кибермошенничества, основанного на социальной инженерии. Звонки от лжесотрудников банков, сообщения о выигрышах, фишинговые письма, маскирующиеся под обращения госорганов, — всё это стало повседневной рутинной. Эффективность таких атак зиждется не на технической сложности, а на манипуляции человеческими эмоциями: страхом, доверчивостью, жадностью или невнимательностью. Статистика МВД по КБР за 2024 год красноречиво свидетельствует о масштабе проблемы: зарегистрировано 45 краж с банковских счетов (рост на 64,4%) и 119 случаев дистанционного мошенничества. Как отмечают в ведомстве, ключевой причиной является низкая цифровая грамотность, особенно среди граждан пожилого и среднего возраста. На другом уровне, менее заметном для обывателя, но критически важном для экономики, находятся угрозы, связанные с компьютерным пиратством и нарушением интеллектуальных прав. Использование

нелицензионного программного обеспечения на предприятиях создает не только правовые риски, но и серьёзные бреши в безопасности, превращая такие системы в легкую мишень для внедрения вредоносных программ. Противодействие этим правонарушениям требует от сотрудников МВД не только знания соответствующих статей Уголовного кодекса РФ (например, ст. 146 «Нарушение авторских и смежных прав»), но и глубокой экспертизы в области IT-инфраструктуры. Наиболее опасным вызовом являются целевые атаки на критическую информационную инфраструктуру. Объекты энергетики, связи, транспорта и финансового сектора республики потенциально могут стать мишенью для высококвалифицированных злоумышленников, включая группы, действующие в интересах иностранных государств. Цель таких атак, классифицируемых как Advanced Persistent Threat, — не сиюминутная выгода, а длительное скрытое присутствие в системах для сбора данных, саботажа или дестабилизации в ключевой момент. Противодействие этим угрозам регулируется отдельными статьями Уголовного кодекса (ст. 274.1) и требует тесной координации с федеральными центрами и спецслужбами.

Ответом на этот комплекс угроз стала адаптивная, многослойная стратегия МВД по КБР, построенная по принципу глубокой эшелонированной обороны. В арсенале современного полицейского, недавно наполненном классическими методами сыска, сегодня появились инструменты, которые еще вчера казались уделом научной фантастики. Основу этой технологической революции составляет планомерное внедрение систем искусственного интеллекта и анализа больших данных. Уже сейчас алгоритмы машинного обучения, работая в режиме реального времени, непрерывно прочесывают цифровое пространство республики. Они автоматически выявляют вновь созданные фишинговые сайты, которые мимикрируют под страницы банков или государственных порталов, отслеживают подозрительные цепочки финансовых транзакций, выстраивая

схемы движения денег, и анализируют поведенческие паттерны пользователей в социальных сетях, чтобы спрогнозировать и пресечь новые, только формирующиеся схемы мошенничества. Параллельно совершил качественный скачок и такой важнейший инструмент, как цифровая криминалистика. Теперь восстановление данных, намеренно удаленных преступником, анализ скрытой метаинформации файлов, которая может указать на авторство или источник, и установление неочевидных связей между разрозненными цифровыми артефактами — от переписки в мессенджерах до записей в логах серверов — стали рутинной, но высокотехнологичной частью стандартной процедуры расследования. В ведомстве все чаще звучит мнение, что будущее всей правоохранительной деятельности неразрывно связано с развитием этих интеллектуальных систем. Только они способны справиться с гигантскими массивами информации, обрабатывая их с такой скоростью и точностью, которая недоступна человеческим возможностям, превращая неструктурированный цифровой шум в четкие улики и доказательную базу. МВД по Кабардино-Балкарии сделало стратегическую ставку на превентивную работу и массовое цифровое просвещение. Вместо того чтобы лишь констатировать факты свершившихся обманов, ведомство перешло к тактике активного опережения. Эта работа вышла за стены кабинетов и приобрела живой, диалоговый характер. Специалисты регулярно встречаются со студентами и школьниками, работниками предприятий и госслужащими в районных администрациях. Суть этих встреч — не формальные лекции, а практические мастер-классы по цифровой безопасности. На свежих, актуальных примерах, взятых из реальной следственной практики республики, людям показывают, как выглядит звонок от лже-сотрудника банка, как отличить поддельное SMS от настоящего и почему не стоит переходить по подозрительным ссылкам в письмах. Гражданам дают не абстрактные наставления, а конкретные, применимые здесь и сейчас инструменты: как создать и запомнить по-

настоящему надежный пароль, как проверить настройки конфиденциальности в социальной сети, чтобы личные данные не стали достоянием мошенников, и какие правила соблюдать при онлайн-покупках или денежных переводах. Эта кропотливая, системная работа направлена на фундаментальную цель — изменить само восприятие риска. Каждый житель республики должен перестать быть пассивной потенциальной жертвой, превратившись в осознанного, бдительного и грамотного союзника правоохранительных органов, в первую, самую важную линию обороны коллективной цифровой безопасности

Эффективность даже самых передовых технологий и масштабных профилактических кампаний сводится к нулю без команды высококвалифицированных специалистов, способных ими управлять, анализировать данные и принимать решения. Ключевым элементом кадровой стратегии МВД по КБР стало стратегическое партнёрство с главным научно-образовательным центром республики — Кабардино-Балкарским государственным университетом. Это сотрудничество выходит за рамки формальностей: эксперты ведомства напрямую участвуют в учебном процессе, помогая формировать новое поколение IT-криминалистов и аналитиков кибербезопасности, уже на студенческой скамье знакомых с реалиями оперативной работы. Для действующих сотрудников выстроена гибкая система непрерывного профессионального роста — регулярные семинары с привлечением ведущих экспертов, курсы повышения квалификации по новым методам расследования и стажировки, позволяющие оставаться на острие технологического прогресса.

Однако в современной борьбе с киберугрозами, которые не признают ведомственных границ, даже самая сильная команда не может действовать изолированно. Понимание этого привело к тому, что межведомственная и межсекторная кооперация стала не просто полезным инструментом, а краеугольным камнем всей оборонительной стратегии. МВД по КБР создало

и поддерживает оперативные рабочие группы и каналы прямого взаимодействия с ключевыми игроками: Управлением ФСБ по республике, региональным отделением Роскомнадзора, структурами Банка России и техническими службами крупнейших телекоммуникационных операторов. Этот постоянно действующий альянс превращается в единый нервный центр, способный в режиме реального времени обмениваться сигналами о новых схемах мошенничества, координированно блокировать фишинговые сайты и номера, а также проводить сложные совместные операции, где скорость реакции и обмена информацией между различными структурами часто является решающим фактором для успеха.

Деятельность МВД по противодействию киберпреступности осуществляется в рамках строгого правового поля. Базисом служат федеральные законы: № 149-ФЗ «Об информации, информационных технологиях и о защите информации», № 187-ФЗ «О безопасности критической информационной инфраструктуры», а также Глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», предусматривающая ответственность за неправомерный доступ к данным (ст. 272), создание и распространение вредоносных программ (ст. 273) и воздействие на КИИ (ст. 274.1). Однако правовое поле часто отстаёт от технологического прогресса. Использование ИИ для расследования, сбор цифровых доказательств в облачных средах, вопросы юрисдикции при трансграничных атаках — эти и другие вызовы требуют постоянного совершенствования законодательства и методологии криминалистической кибернетики. Противодействие киберпреступности в Кабардино-Балкарии перестало быть узкопрофессиональной задачей IT-специалистов в погонах. Сегодня это системная деятельность по построению цифрового иммунитета всего региона. Стратегия МВД по КБР, основанная на триаде «передовые технологии — просвещённое общество — сильные кадры», демонстрирует комплексный подход к решению проблемы.

Использованные источники:

1. Уголовный кодекс Российской Федерации (ред. от 17.11.2025). Глава 28. Преступления в сфере компьютерной информации. https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/
2. Резников Р. Искусственный интеллект в киберзащите. Аналитическое исследование Positive <https://ptsecurity.com/research/analytics/iskusstvennyi-intellekt-v-kiberzaschite/>
3. Статистические данные и материалы брифинга МВД по Кабардино-Балкарской Республике (2024 г.) о состоянии киберпреступности. <https://07.мвд.рф/news/item/47743372/?year=2024&month=3&day=29>
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». https://www.consultant.ru/document/cons_doc_LAW_220885/
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». https://www.consultant.ru/document/cons_doc_LAW_61798/