Андрей Викторович БОРИСОВ,
доцент кафедры уголовного права Военного университета имени князя Александра Невского Министерства обороны РФ, доктор юридических наук, доцент
av-borisov@mail.ru
123001, Россия, г. Москва, ул. Большая Садовая, д. 14, стр. 1

Киберпреступность на транспорте: состояние и тенденции

Аннотация. *В статье проводится анализ криминологической характеристики киберпреступности на транспорте, рассматривается ее состояние и тенденции ее развития. В контексте глобализации ИКТ стали неотъемлемым элементом функционирования общества, включая транспортную инфраструктуру. Вместе с тем использование ИКТ в транспортной сфере порождает новые вызовы и угрозы, в том числе криминального характера. Данный тезис подтверждается результатами многочисленных исследований, проведенных как отечественными, так и зарубежными специалистами в области кибербезопасности и криминологии. Современные киберугрозы, направленные на обеспечение транспортной безопасности Российской Федерации, требуют комплексного и всестороннего анализа. В связи с этим автором статьи предпринята попытка определения количественных и качественных параметров киберпреступности в транспортной сфере, а также выявления основных тенденций ее развития. В рамках исследования проведен анализ положений криминологических работ, посвященных как теоретическим аспектам противодействия киберпреступности, так и практическим вопросам обеспечения транспортной безопасности. Кроме того, была изучена ведомственная статистическая отчетность Министерства внутренних дел Российской Федерации за период с 2018 по 2024 г.*

Ключевые слова: *транспортная преступность, транспортная безопасность, киберпреступность, киберпреступность на транспорте, состояние киберпреступности на транспорте, показатели киберпреступности на транспорте, тенденции киберпреступности на транспорте*

DOI: 10.17803/2311-5998.2025.129.5.214-220

Andrey V. BORISOV,
Associate Professor of the Department of Criminal Law of the Military University named after the Prince Alexander Nevsky of the Ministry of Defense, Dr. Sci. (Law), Associate Professor
av-borisov@mail.ru
14/1, ul. Bolshaya Sadovaya, Moscow, Russia, 123001

Cybercrime in Transport: Status and Trends

Abstract. *The article is devoted to the criminological characteristics of cybercrime in transport, its state and trends of its development are considered. One of the significant factors influencing the formation and development of*

the digital economy in the Russian Federation is the active introduction of advanced information and telecommunication technologies (hereinafter — ICT) into various sectors of activity. In the context of globalization, ICTs have become an integral part of the functioning of society, including transport infrastructure. At the same time, the use of ICT in the transport sector generates new challenges and threats, including criminal ones. This thesis is supported by the results of numerous studies conducted by both domestic and foreign experts in the field of cybersecurity and criminology. Modern cyber threats aimed at ensuring the transport security of the Russian Federation require a comprehensive and comprehensive analysis. In this regard, the author of the article attempts to determine the quantitative and qualitative characteristics of cybercrime in the transport sector, as well as to identify the main trends in its development. The study analyzes the provisions of criminological works devoted to both theoretical aspects of countering cybercrime and practical issues of ensuring transport security. In addition, the departmental statistical reports of the Ministry of Internal Affairs of the Russian Federation for the period from 2018 to 2024 were studied.

Keywords: *transport crime, transport security, cybercrime, cybercrime in transport, the state of cybercrime in transport, indicators of cybercrime in transport, trends in cybercrime in transport*

Транспорт является фундаментальным элементом экономической и инфраструктурной системы государства. Он обеспечивает оптимизацию управления потоками материальных и нематериальных ресурсов, способствуя доступности отдаленных территорий и концентрации населения в ключевых местностях. Транспортные системы играют значительную роль в активизации экономического роста и выступают стимулятором повышения уровня жизни населения страны. Тем не менее их работа сопряжена с рядом сложных проблем и опасностей. Среди них можно выделить техногенные катастрофы, дорожно-транспортные происшествия, антропогенные катастрофы, загрязнение окружающей среды вредными веществами, повышенный уровень шумового загрязнения, потенциальные угрозы общественной безопасности, включая террористические акты и преступления против личности и собственности[1].

Комплексный анализ криминогенной ситуации в транспортной сфере включает исследование как традиционных преступных деяний, свойственных данной области, так и проблем, связанных с киберпреступностью, которая демонстрирует волнообразную динамику в рассматриваемый период. Согласно официальным данным статистического учета, в 2024 г. было зарегистрировано 6 502 случая киберпреступлений, что на 4,9 % меньше по сравнению с прошлым годом[2]. Несмотря на снижение количества киберпреступлений, отмечается увеличение их

[1] *Борисов А. В.* Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета РФ. 2024. № 3 (41). С. 37—44.

[2] *Борисов А. В.* Криминологическая профилактика транспортной преступности // Вестник Академии права и управления. 2019. № 2 (55). С. 30—34.

Рис. 1. Динамика и доля киберпреступлений, совершенных на транспорте в Российской Федерации в 2018—2024 гг.[3]

Рис. 2. Структура (по степени тяжести) киберпреступлений, совершенных на транспорте в Российской Федерации в 2018—2024 гг.

доли в структуре транспортной преступности, которая достигла максимальных значений в рассматриваемый период и составила 22,24 % (рис. 1).

Снижение числа киберпреступлений на транспорте можно объяснить несколькими ключевыми факторами:

— во-первых, разработкой и внедрением комплексных систем киберзащиты, обеспечивающих высокий уровень резистентности к кибератакам. Такие системы минимизируют потенциальные потери от инцидентов и гарантируют способность транспортной организации адекватно реагировать на будущие вызовы в сфере информационной безопасности;

— во-вторых, организацией систематического обучения сотрудников и повышением их осведомленности о новейших методах атак, основанных на социальной инженерии. Это включает в себя анализ поведенческих паттернов злоумышленников и разработку соответствующих контрмер;

— в-третьих, интеграцией механизмов кибербезопасности во все используемые организацией информационные сервисы и продукты. Это предполагает внедрение стандартов информационной безопасности на всех этапах разработки и эксплуатации систем;

— в-четвертых, внедрением и поддержанием процессов управления уязвимостями, включая регулярное обновление систем безопасности и мониторинг потенциальных угроз, что, в свою очередь, позволяет оперативно идентифицировать и устранять слабые места в защите[4].

В 2024 г. в общей массе киберпреступлений, регистрируемых на транспорте, преобладают особо тяжкие деяния. Их удельный вес составляет 48,95 %. Наблюдается тенденция к снижению количества киберпреступлений на транспорте по всем категориям преступных деяний (рис. 2).

---

[3] В статистических формах ГИАЦ МВД России сведения о большинстве киберпреступлений, в том числе совершаемых на транспорте, выделяются с 2018 г. Здесь и далее использовалась форма ведомственной статистической отчетности № 494 «Сведения о состоянии преступности и результатах расследования преступлений» за 2018—2024 гг.

[4] *Борисов А. В.* Состояние и основные тенденции развития преступности на объектах транспорта Российской Федерации // Расследование преступлений: проблемы и пути их решения. 2019. № 2 (24). С. 42—49.

В перечне часто встречающихся киберпреступлений, совершенных на объектах транспортной инфраструктуры в 2024 г., выделяются следующие виды: кражи — 294, разнообразные виды мошенничества — 494, а также преступные деяния, связанные с незаконным оборотом наркотических средств — 4 922.

Киберпреступления в транспортной сфере совершались в 2024 г. следующими основными способами: использование информационно-телекоммуникационной сети Интернет — 5 964 деяния (91,73 %); применение средств мобильной связи — 2 161 деяние (33,24 %); использование программных средств — 1 147 (17,64 %); применение платежных инструментов в виде расчетных (пластиковых) карт — 386 (5,93 %); использование компьютерной техники — 246 (3,78 %); осуществление фиктивных электронных платежей — 20 деяний (0,31 %).

Внедрение информационных технологий в транспортную отрасль способствует значительному повышению эффективности функционирования транспортных систем. Это выражается в оптимизации процессов управления, снижении временны́х и ресурсных затрат, а также в повышении общей производительности транспортных систем. Кроме того, внедрение информационных технологий открывает новые перспективы для всех участников и пользователей в транспортной отрасли, способствуя инновациям и развитию.

Научные исследования, посвященные применению кибертехнологий в транспортной сфере, направлены на унификацию процессов обработки и транспортировки грузов и пассажиров. В рамках этих исследований разрабатываются алгоритмы и системы, обеспечивающие оптимизацию логистических цепочек и повышение безопасности перевозок[5]. Кроме того, ведется работа по созданию единых международных стандартов уровня шума в различных странах. В то же время разрабатывается и внедряется система законов и правил, которые регулируют использование беспилотных транспортных средств. Это создает основу для широкого применения не только автономных наземных транспортных средств, таких как автомобили и электропоезда, но и более компактных и специализированных беспилотных летательных аппаратов.

Современные беспилотные транспортные системы, включая воздушные, наземные и водные, представляют собой передовые технологии, обладающие значительным потенциалом для применения в различных сферах, однако они также сопряжены со следующими потенциальными рисками и угрозами для транспортной безопасности:

1) уязвимость к кибератакам. Беспилотные транспортные средства, не оснащенные адекватными средствами киберзащиты, могут стать целями для злоумышленников. Возможность несанкционированного доступа к управлению такими системами создает риски их использования в террористических или иных преступных целях;
2) риски, связанные с отказом оборудования. Сбои в работе ключевых компонентов беспилотных транспортных систем могут привести к их неконтролируемому поведению, что представляет угрозу для жизни и здоровья людей, а также для инфраструктуры;

[5] *Варыгин А. Н.* Особенности преступности на железнодорожном транспорте // Проблемы правоохранительной деятельности. 2017. № 3. С. 62—65.

3) нарушение воздушного пространства. Беспилотные летательные аппараты могут проникать в контролируемые зоны воздушного пространства, создавая потенциальные помехи для полетов пилотируемых воздушных судов. Это может угрожать безопасности воздушного движения и приводить к нарушению установленных процедур и регламентов.

В современных условиях беспилотные транспортные средства (БТС) являются значимым компонентом киберпространства и вносят существенный вклад в формирование актуальных киберугроз. Интеграция БТС в транспортные системы требует комплексного подхода к обеспечению безопасности и киберзащиты[6].

Особую опасность представляет несанкционированный запуск беспилотных летательных аппаратов в непосредственной близости от авиационных объектов, таких как аэродромы, вертодромы и посадочные площадки. Подобные инциденты могут привести к нарушению процедур обеспечения безопасности полетов, а также вызвать угрозу жизни и здоровью людей. Кроме того, возможны повреждения объектов транспортной инфраструктуры.

В подавляющем большинстве случаев нарушения использования воздушного пространства совершаются владельцами беспилотных летательных аппаратов с взлетной массой, не превышающей 30 килограммов. Такие аппараты, как правило, применяются в личных целях.

Основные причины данных нарушений включают:

— недостаток осведомленности о нормативных правовых актах, регулирующих использование воздушного пространства Российской Федерации;
— недооценка потенциальных рисков и опасностей, ассоциированных с эксплуатацией беспилотных летательных аппаратов;
— отсутствие обязательной регистрации воздушных судов в соответствии с действующими законодательными актами, а также отсутствие надлежащих сертификатов, подтверждающих соответствие эксплуатантов и воздушных судов требованиям к летной годности, создает значительные риски для обеспечения безопасности полетов.

В настоящее время беспилотные летательные аппараты, производимые такими крупными компаниями, как DJI и Parrot, оснащены системами, ограничивающими их полеты в зонах с высокой аэронавигационной активностью, например, над аэродромами. Однако киберпреступниками разработаны методы обхода данных ограничительных систем.

После начала специальной военной операции на территории Украины была проведена продуктивная работа по внесению изменений в нормативные правовые акты, регламентирующие порядок использования воздушного пространства Российской Федерации, и по использованию беспилотных летательных аппаратов. В ходе СВО стало очевидно, насколько значимой и необходимой является такая деятельность. В рамках СВО противник активно использует беспилотные летательные и надводные аппараты для атак на объекты транспортной инфраструктуры Российской Федерации. Так, в Севастополе 29.10.2022 была совершена

[6] *Коимшиди Г. Ф., Саркисян А. Ж.* Прогноз динамики преступности в Российской Федерации на 2020 год // Вестник Академии Следственного комитета Российской Федерации. 2020. № 1 (23). С. 68—77.

атака на военные корабли Черноморского флота и гражданские суда с использованием надводных беспилотных аппаратов. Согласно информации Министерства обороны РФ, теракт был организован 73-м специальным центром морских операций Вооруженных сил Украины. 02.11.2022 Президент Украины Владимир Зеленский заявил о своем намерении создать флот морских беспилотных аппаратов[7].

Результатом работы по противодействию беспилотным летательным и надводным аппаратам стало принятие Федерального закона от 04.08.2023 № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[8], который расширил круг субъектов противодействия беспилотным летательным и надводным аппаратам и наделил их соответствующими полномочиями.

Применение беспилотных летательных аппаратов в противоправных целях является серьезной угрозой для общественной безопасности и государственного устройства. Данные устройства могут быть задействованы для осуществления террористических атак на объекты транспортной инфраструктуры (что, собственно, активно и происходит в период проведения СВО), незаконного оборота оружия, включая его компоненты и боеприпасы, а также для перевозки отравляющих веществ.

Кроме того, БПЛА могут использоваться для сбора и передачи информации. Развитие информационных технологий, в том числе применение БПЛА, привело к возникновению новых форм терроризма, таких как кибертерроризм и биотерроризм. В соответствии с приказом Минтранса России № 52, ФСБ России № 112, МВД России № 134 от 05.03.2010 «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств», угрозы террористического характера классифицируются как потенциальные угрозы, способные привести к актам незаконного вмешательства в деятельность указанных объектов[9].

Беспилотный транспорт является многообещающим вектором развития транспортной отрасли. Однако для успешной интеграции беспилотных транспортных средств необходима комплексная модернизация дорожно-транспортной и информационно-телекоммуникационной инфраструктуры. Эта инфраструктура должна предоставлять беспилотным транспортным средствам актуальные данные и обеспечивать функционирование необходимых сервисов. Вместе с тем научные исследования указывают на потенциальные риски, связанные с внедрением интеллектуальных транспортных систем. Эти угрозы связаны с наличием уязвимостей в программном обеспечении и в каналах передачи данных. Наличие таких уязвимостей может создать условия для осуществления потенциальных кибератак на транспортные системы.

Таким образом, анализ статистических данных о зарегистрированных преступных деяниях, совершенных с использованием информационно-телекоммуникационных

[7] Проект федерального закона № 323987-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» (ред., внесенная в Государственную Думу, текст по состоянию на 28.03.2023) // СПС КонсультантПлюс.

[8] Российская газета. 09.08.2023. № 175.

[9] *Диканова Т. А.* О состоянии преступности на железнодорожном, водном и воздушном транспорте в 2015—2019 гг. // Транспортное право и безопасность. 2020. № 2 (34). С. 84—99.

технологий на транспорте, позволяет сделать определенные выводы. Исследование показывает, что уровень киберпреступности в рассматриваемой сфере подвержен волнообразной динамике.

В структуре киберпреступности на транспорте в 2024 г. доминировали особо тяжкие преступные деяния. Их доля составила 48,95 %. С использованием информационно-телекоммуникационных технологий на транспорте совершались преступные деяния, связанные с незаконным оборотом наркотиков (4 922), различные виды мошенничества (494) и кражи (294). Характерными способами совершения киберпреступлений на транспорте стали использование сети Интернет — 5 964 преступления (91,73 %), использование мобильной связи — 2 161 (33,24 %), применение программных средств — 1 147 преступлений (17,64 %).

БИБЛИОГРАФИЯ

1. *Борисов А. В.* Криминологическая профилактика транспортной преступности // Вестник Академии права и управления. — 2019. — № 2 (55). — С. 30—34.
2. *Борисов А. В.* Состояние и основные тенденции развития преступности на объектах транспорта Российской Федерации // Расследование преступлений: проблемы и пути их решения. — 2019. — № 2 (24). — С. 42—49.
3. *Борисов А. В.* Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета Российской Федерации. — 2020. — № 1. — С. 43—51.
4. *Борисов А. В.* Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета Российской Федерации. — 2024. — № 3 (41). — С. 37—44.
5. *Варыгин А. Н.* Особенности преступности на железнодорожном транспорте // Проблемы правоохранительной деятельности. — 2017. — № 3. — С. 62—65.
6. *Диканова Т. А.* О состоянии преступности на железнодорожном, водном и воздушном транспорте в 2015—2019 годах // Транспортное право и безопасность. — 2020. — № 2 (34). — С. 84—99.
7. *Коимшиди Г. Ф., Саркисян А. Ж.* Прогноз динамики преступности в Российской Федерации на 2020 год // Вестник Академии Следственного комитета Российской Федерации. — 2020. — № 1 (23). — С. 68—77.
8. Официальная статистика Министерства внутренних дел Российской Федерации // URL: https://xn--b1aew.xn--p1ai/reports (дата обращения: 30.03.2025).
9. Промышленный интернет вещей : доклад. — М. : Агентство промышленного развития Москвы, 2020.