

УДК 353

***ЦИФРОВЫЕ ИНСТРУМЕНТЫ УПРАВЛЕНИЯ МЕЖРЕГИОНАЛЬНЫМИ
РЕСУРСАМИ ДЛЯ МИНИМИЗАЦИИ РИСКОВ ТЕРРОРИСТИЧЕСКИХ
УГРОЗ***

Трубин Д.Д.,

студент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Субботина Т.Н.,

к.п.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация

В данной работе анализируется современная экосистема цифровых инструментов управления межрегиональными ресурсами, направленная на минимизацию террористических угроз в Российской Федерации. Рассматриваются ключевые государственные платформы, такие как СМЭВ для оперативного межведомственного обмена данными, ГАИС «ЭРА-ГЛОНАСС» для мониторинга транспорта и идентификации беспилотных воздушных судов. Исследуются причины уязвимости межрегиональной инфраструктуры и её привлекательность для террористических атак в силу высокой стратегической ценности и экономического эффекта. Уделено внимание барьерам правового регулирования.

Ключевые слова: антитеррористическая безопасность, цифровая трансформация, межрегиональные ресурсы, критическая информационная инфраструктура, правовое регулирование.

***DIGITAL TOOLS FOR MANAGING INTERREGIONAL RESOURCES TO
MINIMIZE THE RISKS OF TERRORIST THREATS***

Trubin D.D.,

student,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Subbotina T.N.,

PhD, Associate Professor,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Abstract

This paper analyzes the modern ecosystem of digital tools for managing interregional resources aimed at minimizing terrorist threats in the Russian Federation. Key government platforms are being considered, such as SMEV for operational interdepartmental data exchange, ERA-GLONASS GIS for transport monitoring and identification of unmanned aircraft. The reasons for the vulnerability of the interregional infrastructure and its attractiveness for terrorist attacks due to its high strategic value and economic impact are investigated. Attention is paid to the barriers of legal regulation.

Keywords: anti-terrorist security, digital transformation, interregional resources, critical information infrastructure, legal regulation.

Межрегиональная инфраструктура, как транспортные узлы, энергетические сети, магистральные трубопроводы, является приоритетной целью для террористических атак в силу своей критической значимости для жизнеобеспечения страны и высокого потенциала дестабилизации общества.

Атаки на энергетические и транспортные объекты нацелены на подрыв
Дневник науки | www.dnevnikaui.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

энергетической безопасности и нарушение логистических цепочек, что влечет за собой масштабный экономический ущерб. Многие объекты инфраструктуры, в особенности линейные, такие как ЛЭП или железные дороги, характеризуются географической удаленностью и сложностью обеспечения сплошной охраны на всём протяжении. Современные объекты сильно зависят от ИТ-систем. Недостаточный уровень цифровой защиты и отсутствие полного учета ИТ-активов создают возможности для кибердиверсий. Так, по информации ФСТЭК лишь 36% организаций достигают минимально необходимого уровня защиты от киберугроз [20].

История и современная практика фиксируют случаи атак на ключевые узлы связи, транспорта и энергетики. В 2025 году в ночь с 31 мая на 1 июня произошли подрывы опор автомобильного моста в Брянской области и железнодорожного моста в Курской области [6]. В 2011 году произошёл взрыв в зале международных перелётов в аэропорту Домодедово [15]. В 2022 году был нанесён ракетный удар с использованием вертолетов по нефтебазе «Роснефти» в Белгороде, приведший к возгоранию восьми резервуаров с топливом [16]. На примере ударов по нефтехранилищам и нефтеперерабатывающим заводам особенно хорошо видно, как диверсионная деятельность способна нарушать деятельность отдельных секторов экономики [8]. Повреждение уникального инфраструктурного объекта как крымский мост в октябре 2022 года привело к его перекрытию и невозможности использования на полгода [21].

Текущая система по управлению антитеррористическими ресурсами построена на иерархии между компетенцией федерации и её региональными субъектами. Центральное место в системе занимает Национальный антитеррористический комитет (НАК), руководство которым осуществляет директор Федеральной службы безопасности [17]. На уровне каждого региона функционируют антитеррористические комиссии (АТК), возглавляемые главами субъектов [2]. В такой системе цифровые ресурсы выступают в роли связующего звена между субъектами власти. Цифровой функционал представлен в таблице 1.

Дневник науки | www.dnevnika.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

Таблица 1 - Распределение цифровых ресурсов по антитеррористической деятельности между органами власти

Уровень управления	Орган власти	Цифровой функционал
Федеральный уровень	НАК	Стратегическое планирование, координация межведомственной информации
Уровень субъектов	АТК	Управления региональными ресурсами, применение местных систем мониторинга
Технологический оператор	Минцифры, ФСБ, МВД	Эксплуатация государственных ИС, обеспечение защищённой связи
Финансовый контроль	Росфинмониторинг	Цифровой мониторинг каналов финансирования

На сегодняшний день в России цифровая экосистема управления межрегиональными ресурсами для минимизации террористических угроз представляет из себя сложную структуру. Она объединяет инструменты жесткого контроля (ЭРА-ГЛОНАСС, системы «Поток», «Купол»), механизмы оперативного взаимодействия (СМЭВ, Система-112), платформы идентификации (ГИС ЕБС) и средства финансового мониторинга (Прозрачный блокчейн).

На федеральном уровне для межведомственного обмена информацией используют Систему межведомственного электронного взаимодействия (СМЭВ) [11]. Данной системой пользуются не только правоохранительные органы, так как она в целом предназначена для исполнения и оказания государственных услуг. В контексте антитеррористической деятельности СМЭВ позволяет правоохранительным органам мгновенно верифицировать личности, проверять транспортные средства и отслеживать перемещения подозреваемых лиц между регионами.

Альтернативный способ межведомственной координации, это Система-112. Особенностью этой системы по сравнению с СМЭВ является упор на дежурно-диспетчерские службы полиции, скорой помощи, пожарной охраны и службы «Антитеррор» [10]. Помимо удобного способа принятия сообщений в одном окне, система автоматически определяет местоположение звонящего.

Для обеспечения безопасности и контроля транспортной инфраструктуры применяют ГАИС «ЭРА-ГЛОНАСС» [1]. Изначально, при запуске системы в 2015 году, её позиционировали как средство для экстренного реагирования при авариях. Техническая составляющая системы, однако, позволяет проводить более широкий мониторинг. Для антитеррористических целей система позволяет отслеживать через дорожные камеры наблюдения трек движения конкретного транспортного средства, шифровать полученную информацию и передавать экстренную информацию в приоритетном порядке через любого доступного сотового оператора [19]. Помимо транспортного контроля «ЭРА-ГЛОНАСС» умеет отслеживать БПЛА в силу своего большого географического покрытия [3].

Для узкоспециализированного поиска транспортных средств и быстрого реагирования оперативно розыскных подразделений была разработана АПК «Поток-М» [12]. Камеры мобильных автобусов автоматически считывают номерные знаки автомобилей и сверяют с базами розыска МВД, ФСБ и ФТС. Данные от комплексов собирают в центрах обработки данных, которые взаимодействуют с федеральными информационными массивами и аппаратно-программным комплексом (АПК) «Безопасный город». Таким образом «Поток-М» является удобным инструментом для пресечения логистики террористических групп.

Минимизация рисков на уровне населенных пунктов обеспечивается через АПК «Безопасный город». «Безопасный город» — это программный комплекс, который позволяет реагировать на происшествия и прогнозировать возможные угрозы. К системе имеют доступ МЧС, МВД и ФСБ. Система умеет выявлять подозрительные действия и оставленные предметы, разыскивать транспорт и

Дневник науки | www.dnevnika.ru | СМЭ ЭЛ № ФС 77-68405 ISSN 2541-8327

позволяет взаимодействовать совместно муниципальным и правоохранительным органам. Например, в Москве на 2024 год установлено примерно 225 тыс. камер наружного наблюдения [5].

Ещё одно направление, это развитие систем биометрии для доступа в цифровые системы или физические места. Использование биометрических характеристик (лицо, голос) позволяет повысить уровень защищенности объектов критической инфраструктуры. Например, в Москве внедрены требования по использованию ЕБС для контроля доступа на строительные площадки в целях повышения их антитеррористической защищенности [7].

В ответ на возрастающие риски использования дронов в террористических целях в России разработана система «Купол» [4]. Этот программно-аппаратный комплекс использует алгоритмы искусственного интеллекта для обнаружения и нейтрализации беспилотных летательных аппаратов. Система ищет и отличает БПЛА от других воздушных объектов и уже используется на промышленных предприятиях. Стоит оговориться, что так как система использует военную инфраструктуру, то доступ к ней есть у Министерства обороны РФ [9].

Ключевым направлением развития на ближайшие годы станет углубление интеграции этих систем на базе СМЭВ, что позволит силовым структурам работать не с копиями баз данных, а в режиме реального времени. Внедрение искусственного интеллекта во все звенья цепи: от видеоаналитики в АПК «Безопасный город» до анализа блокчейн-транзакций. Это позволит автоматизировать процесс выявления угроз, снижая нагрузку на операторов и повысит точность прогнозирования.

Правовое регулирование цифровой защиты указанной инфраструктуры встречает ряд проблем, связанных с неточной квалификацией угроз, терминов и технологическим переходом. Например, под АПК «Безопасный город» понимают совокупность специальных технических и функциональных требований, но единого термина что представляет собой «Безопасный город» нет [13]. Это приводит к тому, что в субъектах программу реализуют по-разному – иногда это

Дневник науки | www.dnevnika.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

просто видеонаблюдение. Так, в Калужской области 3 из 5 городов, оснащённых этой системой, имеют суммарно 5 камер на общее население 175 000 человек [14]. Также отсутствует Федеральный Закон, который регламентировал бы деятельность исполнительных органов субъектов РФ по построению и развитию комплекса, а также четкое взаимодействие ведомств между собой, так как АПК имеет статус концепции.

С 1 сентября 2025 года вступили в силу изменения в Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ)» [18]. Статья 10.1 устанавливает прямой запрет на использование иностранных программных компонентов в значимых объектах КИИ при наличии российских аналогов. Для операторов систем проблема заключается в возможности доказать, что замена технически невозможна, так как отсутствуют критерии такой невозможности и правовые последствия отказа.

Таким образом можно сделать вывод, что Россия обладает передовой технической базой для цифровой защиты ресурсов. Для полной реализации этого потенциала необходимо завершить федерализацию правовых норм, особенно в части городского мониторинга, обеспечить импортозамещение в КИИ и повысить квалификацию персонала, отвечающего за эксплуатацию интеллектуальных систем безопасности, а также рассмотреть возможность объединить указанные системы на базе СМЭВ.

Библиографический список:

1. "Методические рекомендации по проведению эксперимента по обеспечению электронного взаимодействия участников процесса перевозок пассажиров автомобильным транспортом по межрегиональным маршрутам регулярных перевозок" (утв. Минтранс России 14.01.2026) // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

2. "Положение об антитеррористической комиссии в субъекте Дневник науки | www.dnevnika.ru | СМИ ЭЛ № ФС 77-68405 ISSN 2541-8327

Российской Федерации" (утв. НАК 17.06.2016) // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

3. «ЭРА-ГЛОНАСС» готова выполнить функцию единой системы идентификации БПЛА // Официальный сайт ФГБУ «РФИ Миприроды России» [Электронный ресурс]. – URL: <https://rfi.mnr.gov.ru/news/news-rfi/era-glonass-gotova-vypolnit-funktsiyu-edinoy-sistemy-identifikatsii-bpla> (дата обращения: 10.04.2026).

4. В РФ разработали систему для защиты предприятий от дронов с ИИ "Купол" // ИА ТАСС [Электронный ресурс]. – URL: <https://tass.ru/armiya-i-opk/23105197> (дата обращения: 10.04.2026).

5. Видеонаблюдение в Москве // TRADVISER [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82:%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D0%B1%D0%BB%D1%8E%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2_%D0%9C%D0%BE%D1%81%D0%BA%D0%B2%D0%B5 (дата обращения: 10.04.2026).

6. Главное об обрушение моста и катастрофа поезда в Брянской области // Коммерсантъ [Электронный ресурс]. – URL: <https://www.kommersant.ru/doc/7773744> (дата обращения 19.04.2026)

7. Единая биометрическая система на объектах строительства (РС ЕБС) // GlobalCIO [Электронный ресурс]. – URL: <https://globalcio.ru/projects/54522/> (дата обращения: 10.04.2026).

8. Минэнерго объяснило мораторий на обнуление топливного демпфера // РБК [Электронный ресурс]. – URL: <https://www.rbc.ru/rbcfreenews/68ebf0e09a79472e85c77124?from=newsfeed> (дата обращения 19.04.2026)

9. Партнёры // АО «Русский Купол» [Электронный ресурс]. – URL: Дневник науки | www.dnevnikaui.ru | СМИ ЭЛ № ФС 77-68405 ISSN 2541-8327

<https://xn----otbcdcdguhdkawh.xn--p1ai/page/o-kompanii> (дата обращения: 10.04.2026).

10. Постановление Правительства РФ от 21.11.2011 N 958 (ред. от 20.11.2018) "О системе обеспечения вызова экстренных оперативных служб по единому номеру "112" (вместе с "Положением о системе обеспечения вызова экстренных оперативных служб по единому номеру "112") // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

11. Постановление Правительства РФ от 8 сентября 2010 г. N 697 "О единой системе межведомственного электронного взаимодействия" // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

12. Поток-М – аппаратно-программный комплекс «Поток» // Официальный сайт «РОССИ» [Электронный ресурс]. – URL: <https://rossi-potok.ru/ru/products/potok-m#> (дата обращения: 10.04.2026).

13. Распоряжение Правительства РФ от 03.12.2014 N 2446-р Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город" // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

14. РИП АПК "Безопасный город" // Официальный сайт Правительства Калужской области [Электронный ресурс]. – URL: <https://digital.admoblkaluga.ru/page/bezopasnyy-gorod/> (дата обращения: 10.04.2026).

15. Теракт в «Домодедово» в 2011 году : хронология, пострадавшие, виновные // Lenta.ru [Электронный ресурс]. – URL: <https://lenta.ru/articles/2026/01/24/terakt/> (дата обращения 19.04.2026)

16. Удар вертолётов ВСУ по нефтебазе в Белгороде. Причины и последствия // РБК [Электронный ресурс]. – URL: <https://rostov.rbc.ru/politics/01/04/2022/6247166a9a7947740af8d546> (дата Дневник науки | www.dnevniknauki.ru) СМИ ЭЛ № ФС 77-68405 ISSN 2541-8327

обращения 19.04.2026)

17. Указ Президента РФ от 15.02.2006 N 116 "О мерах по противодействию терроризму" (вместе с "Положением о Национальном антитеррористическом комитете") // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

18. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

19. Федеральный закон "О Государственной автоматизированной информационной системе "ЭРА-ГЛОНАСС" от 28.12.2013 N 395-ФЗ // СПС КонсультантПлюс [Электронный ресурс]. – URL: <https://www.consultant.ru> (дата обращения: 10.04.2026).

20. ФСТЭК: только треть критической инфраструктуры достигла минимального уровня киберзащиты // Коммерсантъ [Электронный ресурс]. – URL: <https://www.kommersant.ru/doc/8380028> (дата обращения 19.04.2026).

21. Хуснуллин сообщил, что восстановление Крымского моста идет по графику // ИА ТАСС [Электронный ресурс]. – URL: <https://tass.ru/ekonomika/18586795> (дата обращения 19.04.2026)