УДК: 351.74/75+34.031.5

Особенности организации охраны объектов подразделениями вневедомственной охраны войск национальной гвардии в условиях цифровой трансформации

Specifics of organizing facility security by the National Guard non-departmental security units in the context of digital transformation

А.В. Шипулин© **A.V. Shipulin©**
Главное управление вневедомственной охраны Росгвардии, г. Москва, Российская Федерация
E-mail: ShipulinAV@rosgvard.ru

Аннотация. В статье рассмотрены особенности организации деятельности подразделений вневедомственной охраны войск национальной гвардии Российской Федерации по обеспечению охраны объектов в условиях цифровизации и цифровой трансформации. Обобщены основные направления цифровизации и цифровой трансформации, реализуемые в Росгвардии, и на этой основе предложены пути совершенствования организации охраны объектов. Отдельное внимание уделено возможностям применения технологий искусственного интеллекта, цифровых двойников, OSINT-поиска, а также систем оптимизации и поддержки принятия управленческих решений в рассматриваемой сфере.

Abstract. The article examines the organizational features of the non-departmental security units of the National Guard of the Russian Federation in ensuring facility protection within the context of digitalization and digital transformation. The study summarizes the primary directions of digitalization and digital transformation implemented within Rosgvardia, and on this basis, proposes methods for improving the organization of facility security. Particular attention is paid to the potential applications of artificial intelligence technologies, digital twins, OSINT (Open-Source Intelligence), and systems for optimizing and supporting management decision-making in this field.

Ключевые слова: охрана; особо важные объекты; режимные объекты; безопасность; технические средства охраны; войска национальной гвардии; вневедомственная охрана; цифровая трансформация

Keywords: security; high-importance facilities; restricted-access facilities; safety; technical security systems; National Guard troops; non-departmental security; digital transformation

ДЛЯ ЦИТИРОВАНИЯ: Шипулин А.В. Особенности организации охраны объектов подразделениями вневедомственной охраны войск национальной гвардии в условиях цифровой трансформации // Академический вестник войск национальной гвардии Российской Федерации. – 2026. – № 2. – С. 42–47.

Обеспечение безопасности государства, общества и граждан от противоправных деяний, в том числе защита собственности и имущества граждан и организаций, продолжает оставаться одной из важнейших задач правоохранительных органов. От эффективности реализации этой задачи напрямую зависит стабильность экономического развития государства и благополучие общества.

Федеральная служба войск национальной гвардии Российской Федерации является одной из основных государственных структур, обеспечивающих безопасность в стране. В ее состав входят подразделения вневедомственной охраны, на которые в соответствии с Федеральным законом «О войсках национальной гвардии Российской Федерации» [1] возложен широкий круг задач. К числу основных относятся: охрана «особо важных и режимных объектов>...< подлежащих обязательной охране войсками национальной гвардии>... <имущества физических и юридических лиц по договорам» [1]; а также обеспечение «по решению Президента>...<безопасности высших должностных лиц субъектов>...<руководителей высших исполнительных органов государственной власти субъектов>...<и иных лиц» [1].

Исходя из специфики реализации функции по обеспечению безопасности высших должностных лиц и включения в данное понятие более широкого спектра задач, по сравнению с охраной, в данной статье будет рассмотрена только ее более узкая составляющая – охрана объектов.

В свою очередь все объекты, охраняемые подразделениями вневедомственной охраны, условно можно разделить на две части:

1. Охрана которых предусмотрена различными нормативными правовыми актами: подлежащие обязательной охране войсками национальной гвардии в соответствии с утвержденным Правительством Российской Федерации перечнем [5]; включенные в перечень объектов, на которые частная охранная деятельность не распространяется [3]; в рамках обеспечения антитеррористической защищенности объектов, определенных в отдельных постановлениях Правительства Российской Федерации; предусмотренная иными нормативными правовыми актами (охрана комнат хранения оружия, наркотических и иных ограниченных в обороте веществ и предметов, а также возложенные задачи в рамках исполнения законодательства о защите свидетелей и должностных лиц государственных организаций).

2. Охрана объектов и имущества, принадлежащих иным юридическим и физическим лицам.

Непосредственно охрана объектов осуществляется Центром специального назначения вневедомственной охраны Федеральной службы войск национальной гвардии (далее – ЦСН ВО) и федеральными государственными казенными учреждениями «Управлениями (отделами) вневедомственной охраны по субъектам Российской Федерации» (далее – ФГКУ УВО (ОВО). Необходимые для организации охраны полномочия предусмотрены в положении о ЦСН ВО и уставах ФГКУ УВО (ОВО).

При этом порядок осуществления данной деятельности регулируется ведомственными нормативными актами [6; 7] и большим количеством методических рекомендаций [12].

Вышеобозначенными приказами Росгвардии определены три вида охраны: физическая, техническая и комбинированная. В свою очередь организация данных видов охраны регулируется приказами Росгвардии, определяющими порядок деятельности строевых подразделений полиции и технической службы.

В зависимости от вида объекта охрана организуется в соответствии с правилами, определенными для объектов, подлежащих обязательной охране войсками национальной гвардии [7] и для иных [6] (далее – Правила). Вместе с тем необходимо отметить, что на настоящий момент отсутствуют приказы:

– регулирующие порядок организации безопасности высших должностных лиц субъектов, руководителей высших исполнительных органов государственной власти субъектов и иных лиц;

– охраны объектов и имущества при применении: «отдельных мер>...<в отношении потерпевших, свидетелей>...<иных участников>...<в соответствии с федеральным законом>...<«О государственной защите>...<участников уголовного судопроизводства» [6], а также «отдельных мер государственной защиты судей, должностных лиц правоохранительных>...<контролирующих органов>...<и иных лиц>...<установленных федеральным законом>...<«О государственной защите» [6].

Указанные Правила содержат два раздела, которые в свою очередь можно разделить на следующие стадии:

1. Порядок приема имущества под охрану, включающий в себя: организацию преддоговорной работы (получение заявления (необходимой документации от собственника), обследование, определение видов и способов охраны (согласование их с собственником), работа с проектно-монтажной организацией (включающая в себя согласование и прием технических средств, установленных на объекте, в том числе их технологический прогон), перечень принимаемого под охрану имущества, согласование проекта договора; заключение договора на определенный вид охраны; составление предусмотренной приказом документации; определение ответственных должностных лиц.

2. Охрана имущества: выполнение предусмотренных договором обязательств; взаимодействие с собственником и его ответственными лицами по различным вопросам организации охраны (обследование, вынесение предписаний и их исполнение, предоставление необходимых условий для размещения постов физической охраны, выставление и оплата счетов за оказанные услуги); работа с обслуживающей технические средства охраны организацией (через собственника объекта). Правилами в некоторых случаях предусматривается неполный перечень обозначенных процедур – в зависимости от предмета, вида охраны, а также предусмотренного порядка заключения договора.

Следует отметить, что Правилами предусмотрен контроль за исправностью (работоспособностью) установленных на объекте техническими средствами охраны, вместе с тем четко определенного алгоритма воздействия на собственника при выборе им обслуживающей организации на данный момент нет. При этом надежность технической охраны полностью зависит от качества и полноты организации данной работы. Представляется целесообразным для объектов, безопасность которых важна для государства, разработать механизм получения такими обслуживающими технические средства организациями специальной аккредитации (сертификации).

Проведя анализ развития охраны с помощью технических средств, необходимо отметить, что основной тенденцией является автоматизация процессов и компьютеризация данных систем. С конца 90-х годов XX века автоматизированные рабочие места на базе персональных компьюте-

ров применяются в подразделениях вневедомственной охраны, а на объектах устанавливаются высокотехнологичные извещатели, использующие достижения современной науки и техники.

В свою очередь, разработкой основных направлений возможного применения цифровых технологий в охранной деятельности подразделениями вневедомственной охраны занимается ФКУ «НИЦ «Охрана» Росгвардии [9] (далее – Центр) в рамках проводимых научно-исследовательских и опытно-конструкторских работ.

В этих целях разрабатываются системы: с использованием технологий искусственного интеллекта (аудио- и видеоаналитики), обработки больших данных (для анализа информации, поступающей как от систем передачи извещений, так и от иных средств безопасности – систем контроля доступа, аудио- и видеозаписи, а также технологических и иных систем, установленных на объекте); виртуальной и дополненной реальности – для организации обучения личного состава; основанные на новых принципах обнаружения проникновения на охраняемые объекты (аморфный ферромагнитный микропровод, ситуационная аудио- и видео аналитика, анализатор спектра звука выстрела) и создания на их основе извещателей.

Особого внимания требуют системы предиктивной аналитики, которые должны строиться на основе всего объема информации, поступающей от всех систем обеспечения безопасности, включая технологические [10]. Развитие таких технологий является ключевым этапом цифровой трансформации в охранной деятельности.

Важнейшим элементом создания и выбора оптимальной системы безопасности на объекте является применение технологий цифровых двойников объектов [9], использование которых позволяет оперативно выявлять недостатки в системе безопасности, предлагать варианты усиления защиты, оценивать потенциальные потери на объекте, что в целом позволяет создать оптимальную систему защиты при заданном уровне безопасности.

Помимо перечисленных преимуществ, технологии цифровых двойников охраняемых объектов целесообразно использовать при подготовке паспортов антитеррористической защищенности объектов с последующим их хранением на единой защищенной платформе «ГосТех». Это обеспечит оперативное использование соответствующей информации при планировании и применении сил и средств правопорядка в случае совершения противоправных деяний на объектах.

Использование виртуальной реальности на основе цифровых двойников позволяет проводить тренировки по отработке действий на объекте для подразделений вневедомственной охраны и отрядов специального назначения, в том числе с моделированием чрезвычайных ситуаций и последующей оценкой действий личного состава.

Ещё одним элементом системы безопасности охраняемых объектов должна стать так называемая технология OSINT – система поиска и сбора информации по открытым источникам сети Интернет [8; 11]. Переход (перенос) охранной деятельности в цифровую среду требует разработки комплекса мер, направленных на защиту объектов в цифровом пространстве.

Основным направлением защиты объектов в цифровой сфере должен стать анализ информации о них в сети Интернет, в том числе: выявление противоправных высказываний и призывов в социальных сетях, связанных с охраняемыми объектами; мониторинг запросов, касающихся систем защиты (включая закупки оборудования), а также размещенных в сети схем внутренних помещений и комплексов безопасности; сбор сведений о недобросовестных поставщиках и установщиках систем безопасности, включая организации, осуществляющие обслуживание; выявление информации о базах данных со сведениями об охраняемых объектах, находящихся в открытом доступе вследствие утечек.

Помимо обозначенных задач технологию OSINT можно использовать для проверки контрагентов перед заключением договора (для снижения репутационных рисков и предупреждения дебиторской задолженности).

Все вышеперечисленные перспективные направления в той или иной мере могут быть применены в подразделениях вневедомственной охраны. При этом в рамках разработанной в Росгвардии ведомственной программы цифровой трансформации запланировано проведение мероприятий в двух основных направлениях:

1. Цифровизации деятельности, связанной с созданием и развитием государственной информационной системы в сферах «оборота оружия>...<частной охранной>....< детективной деятельности> ...<вневедомственной охраны>... <федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса>...<деятельностью подразделений охраны юридических лиц с особыми уставными задачами>...<подразделений ведомственной охраны» (далее – ГИС или ФПКО), как ведомственного сегмента управления охранной деятельностью в Российской Федерации [2].

Данная государственная информационная система содержит два больших блока, первый из которых цифровизирует деятельность подразделений лицензионно-разрешительной работы и государственного контроля Росгвардии, а второй связан с созданием цифровой среды организации охраны объектов и направлен на цифровизацию взаимо-

действия подразделений вневедомственной охраны с клиентами. Размещение ФПКО Росгвардии осуществляется на государственной платформе ГосТех [4].

Помимо переноса в цифровой формат служебной деятельности подразделений Росгвардии, основной задачей создаваемой системы государственного управления является цифровая трансформация выполняемых государственных услуг и функций, в результате которой предполагается создание систем интеллектуальной аналитики, оптимизации и поддержки принятия управленчес-ких решений. Создание данной ГИС осуществляется в плановом порядке в рамках согласованных технических заданий.

2. Развития общих сервисов по цифровизации деятельности внутри Росгвардии (систем электронного документооборота, электронной почты, ведения бухгалтерского учета «Витязь», иных ведомственных сервисов и информационных баз данных), а также создание цифровых сервисов в рамках направлений деятельности по профилю каждого подразделения.

При этом необходимо отметить, что документа, планирующего направление профильной организации деятельности подразделений вневедомственной охраны по цифровизации и цифровой трансформации нет. Несмотря на это, в рамках развития охранной деятельности подразделений вневедомственной охраны уже внедрены и используются следующие цифровые сервисы:

1. В ряде ФГКУ УВО (ОВО) для улучшения работы с клиентами используются региональные системы межведомственного документооборота, позволяющие в электронном режиме заключать договоры, выставлять и получать оплату за оказываемые услуги. Данная система также позволяет вести претензионную работу с контрагентами.

2. В 2025 году на региональных сайтах всех ФГКУ УВО (ОВО) внедрены электронные сервисы «Хочу служить в Росгвардии» (для приема на службу), «Заявка на охрану объекта или квартиры» (для подачи соответствующего заявления), «Заявка на проведение обследования и категорирования объекта (территории)» (в рамках антитеррористической защиты объектов, «Тарифы и оплата» (для оплаты через банковские приложения посредством QR-кодов и системы быстрых платежей).

3. Как уже отмечалось ранее, все подразделения в своей деятельности используют автоматизированные рабочие места систем централизованной охраны (системы передачи извещений, оконечные устройства с автоматизированной постановкой-снятием объектов с охраны, ведение электронной базы данных объектов и другие).

Все проводимые мероприятия цифровизации реализуются в рамках единой технической политики в области вневедомственной охраны [12], которая предусматривает установку и использование единых требований к созданию технических средств охраны предприятиями-изготовителями.

С учетом того, что в плановом порядке в рамках создаваемой ФПКО в Росгвардии в цифровой формат будут переведены правоотношения по заключенным договорам, а также основные направления служебной деятельности, далее полагаем целесообразным рассмотреть особенности, которые будут возникать (или уже возникают) при осуществлении охранной деятельности в условиях цифровизации и цифровой трансформации.

Во-первых, происходит объединение сети Интернет и ведомственного сегмента, в результате чего одним из основных вопросов остается защита данных.

Во-вторых, цифровизация процесса приема объекта под охрану требует создания мобильного приложения, используемого инженерно-техническим персоналом при обследовании объекта. В рамках данного сервиса также необходимо в дальнейшем вести речь о функции, позволяющей на основе научно разработанной методики осуществлять выбор наиболее оптимального вида охраны и необходимые при этом технические средства. В продолжение данного вопроса целесообразно проработать возможность нормативного закрепления обязанности собственников осуществлять оцифровку принадлежащих им объектов.

В-третьих, необходимо обеспечить взаимодействие клиентов с подразделениями вневедомственной охраны и организациями, обслуживающими технические средства охраны, посредством электронных сервисов. Причем большинство запросов должно обрабатываться и осуществляться в автоматизированном режиме («мгновенного получения ответа»). Немаловажным также будет являться создание автосекретарей (голосовых помощников).

В-четвертых, требует переработки сложившаяся система взаимодействия подразделений вневедомственной охраны с мониторинговыми компаниями и частными охранными организациями. Так, с нашей точки зрения, необходима разработка для всех субъектов охранной деятельности единых технических требований к используемым техническим средствам охраны, в том числе к и их сертификации.

В-пятых, необходимо нормативное закрепление новых технологий, используемых в охранной деятельности (биометрических данных, технологий искусственного интеллекта (аудио- и видео аналитики), обработки больших данных, цифровых двойников, систем оптимизации и поддержки принятия решений и тому подобных сервисов).

В-шестых, перенос охранной деятельности в цифровой формат требует создания системы за-

щиты от противоправных проявлений, возникающих в сети Интернет. Видится перспективным использование для этих целей технологии OSINT-поиска.

В-седьмых, развитие и использование технических средств (роботизированных комплексов (в том числе беспилотных летательных аппаратов) в преступных целях создает быстроменяющуюся среду противоправных посягательств и без вспомогательных систем, позволяющих оказывать помощь человеку, противодействовать им не представляется возможным. Также системы оказания помощи принятия решений позволяют оптимизировать деятельность по управлению нарядами и служебную деятельность в целом.

Результатом внедрения цифровых сервисов в работу вневедомственной охраны должно стать создание принципиально новой системы (на основе предиктивной аналитики), позволяющей перейти от существующей на данный момент системы «сработка технических средств – реагирование» к системе «прогнозирование – предупреждение – пресечение». Основным способом охраны при этом должен стать прогноз и предупреждение противоправных проявлений на основе анализа данных, получаемых в результате применения технических средств при осуществлении охранной деятельности.

В заключение статьи хочется отметить, что перенос охранной деятельности в цифровой формат потребует технических, организационных и нормативных изменений существующего в настоящий момент порядка. Возникающие в ходе этого особенности напрямую связаны с защитой информации, в первую очередь персональных данных, сведений о виде и способе охраны, схемах организации безопасности охраняемых объектов.

Особое внимание при организации охраны объектов в условиях цифровой трансформации необходимо обратить на изменение подходов работы с клиентами и в первую очередь с мониторинговыми компаниями и частными охранными организациями. При этом важным моментом является своевременное нормативное урегулирование используемых при охране объектов новых технологий, а также регламентация вопросов цифровизации деятельности подразделений вневедомственной охраны.

Несомненно, что решение всех вышеперечисленных в статье проблемных моментов позволит в результате обеспечить более надежную охрану объектам, а также создаст систему государственного управления охранной деятельностью с учетом происходящей цифровой трансформации, что в целом положительно скажется на обеспечении безопасности в стране.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 3 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

2. Постановление Правительства Российской Федерации от 17 апреля 2025 г. № 508 «Об утверждении Положения о государственной информационной системе в сфере оборота оружия, в сфере частной охранной и частной детективной деятельности, в сфере вневедомственной охраны, в сфере федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса, за деятельностью подразделений охраны юридических лиц с особыми уставными задачами и подразделений ведомственной охраны» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

3. Постановление Правительства Российской Федерации от 14 августа 1992 г. № 587 «Вопросы частной детективной (сыскной) и частной охранной деятельности» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

4. Распоряжение Правительства Российской Федерации от 21 октября 2022 г. № 3102-р «Об утверждении Концепции создания и функционирования единой цифровой платформы Российской Федерации «ГосТех», плана мероприятий («дорожной карты») по созданию единой цифровой платформы Российской Федерации «ГосТех» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

5. Распоряжение Правительства Российской Федерации от 15 мая 2017 г. № 928-р «О перечне объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации» // официальный Интернет-портал правовой информации http://pravo.gov.ru (дата обращения: 26.01.2026).

6. Приказ Росгвардии от 28 декабря 2018 г. № 669 «Об утверждении Правил охраны имущества физических и юридических лиц по договорам войсками национальной гвардии Российской Федерации» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

7. Приказ Росгвардии от 27 сентября 2018 г. № 427 «Об утверждении Правил охраны объектов,

подлежащих обязательной охране войсками национальной гвардии Российской Федерации, в соответствии с перечнем, утвержденным Правительством Российской Федерации» // Официальный Интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 26.01.2026).

8. Медведев Д.А., Малыхин А.Е. Направления интеграции инструментов OSINT в процессы обеспечения безопасности предприятий нефтегазового сектора // Социально-политические исследования. – 2025. – №2 (27). – URL: https://cyberleninka.ru/article/n/napravleniya-integratsii-instrumentov-osint-v-protsessy-obespecheniya-bezopasnosti-predpriyatiy-neftegazovogo-sektora (дата обращения: 26.01.2026).

9. Безопасность личности, общества, государства: сборник статей Ведомственной научно-практической конференции (Москва, 30 октября 2024 г.). – М.: Научно-исследовательский центр «Охрана» Росгвардии, 2025. – 147 с. – EDN WRBYTM.

10. Рябцев Н.А. О перспективах применения средств обнаружения техногенных угроз в системах вневедомственной охраны / Н.А. Рябцев, А.Н. Членов // Проблемы техносферной безопасности: материалы Международной научно-практической конференции молодых учёных и специалистов. – 2025. – № 14. – С. 29–32. – EDN DRWUBK.

11. Матросова Л.Д., Кислицин И.А. Инструменты для поиска оперативно-значимой информации по открытым источникам // Научный вестник ОрЮИ МВД России имени В.В. Лукьянова. – 2022. – №4 (93). – URL: https://cyberleninka.ru/article/n/instrumenty-dlya-poiska-operativno-znachimoy-informatsii-po-otkrytym-istochnikam (дата обращения: 26.01.2026).

12. Интернет-сайт ФКУ «НИЦ «Охрана» Росгвардии. – URL: https://nicohrana.ru/#.

Статья проверена программой Антиплагиат. Оригинальность — 78 %.

Статья поступила в редакцию 27.02.2026; одобрена после рецензирования 03.04.2026; принята к публикации 15.05.2026.