

ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНТНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

FORMATION OF PROFESSIONAL COMPETENCE IN THE FIELD OF INFORMATION SECURITY FOR EMPLOYEES OF THE INTERNAL AFFAIRS BODIES OF RUSSIA UNDER CONDITIONS OF DIGITALIZATION

Нечай А.А., канд. пед. наук, доцент кафедры информационной безопасности, Санкт-Петербургский университет МВД России

Алексеева О.В., начальник кабинета специальных дисциплин кафедры математики и информатики, Санкт-Петербургский университет МВД России

Гончар А.А., канд. воен. наук, доцент кафедры информационной безопасности, Санкт-Петербургский университет МВД России

Nechay A.A., Candidate of Pedagogical Sciences, Associate Professor of the Information Security Department, St. Petersburg University of the Ministry of Internal Affairs of Russia

Alekseeva O.V., Head of the Special Disciplines Office, Department of Mathematics and Informatics, St. Petersburg University of the Ministry of Internal Affairs of Russia

Gonchar A.A., Candidate of Military Sciences, Associate Professor of the Information Security Department, St. Petersburg University of the Ministry of Internal Affairs of Russia

В контексте активной цифровизации деятельности государственных структур исследование проблематики формирования профессиональной компетентности в сфере информационной безопасности для сотрудников органов внутренних дел (ОВД) МВД России приобретает критическую важность. Данная статья посвящена анализу специфических требований к компетенциям сотрудников ОВД, обусловленных оперативно-служебными задачами и особым статусом обрабатываемой информации. Авторы акцентируют внимание на необходимости разработки целостной методической системы, интегрирующей правовые, технические и оперативно-тактические аспекты информационной безопасности. В работе выявляются системные пробелы в существующих подходах к подготовке сотрудников ОВД и обосновывается комплекс мер, направленных на совершенствование данного процесса. Методологическую основу составили системный анализ, сравнительно-сопоставительный метод и экспертная оценка. Практическая значимость результатов заключается в разработке прикладных рекомендаций по модернизации учебных программ и внедрению специализированных тренажерных комплексов, моделирующих реальные киберугрозы.

In the context of active digitalization of state structures' activities, researching the formation of professional competence in information security for employees of the Internal Affairs Bodies (IAB) of the Russian Ministry of Internal Affairs becomes critically important. This article analyzes the specific competency requirements for IAB employees, dictated by operational and service tasks and the special status of the information they handle. The authors emphasize the need to develop a holistic methodological system integrating legal, technical, and operational-tactical aspects of information security. The study identifies systemic gaps in existing approaches to training IAB employees and substantiates a set of measures aimed at improving this process. The methodological basis includes system analysis, comparative method, and expert evaluation. The practical significance of the results lies in developing applied recommendations for modernizing educational programs and implementing specialized training simulators that model real cyber threats. The proposed solutions aim to enhance the level of protection of official information and the resilience of the Ministry of Internal Affairs' information infrastructure to modern challenges.

Предложенные решения нацелены на повышение уровня защищенности служебной информации и устойчивости информационной инфраструктуры МВД к современным вызовам.

Ключевые слова: профессиональная компетентность, информационная безопасность, органы внутренних дел, цифровая трансформация, защита служебной информации, киберугрозы, подготовка кадров.

Для цитирования: Нечай А.А., Алексеева О.В., Гончар А.А. Формирование профессиональной компетентности в области информационной безопасности сотрудников органов внутренних дел России в условиях цифровизации // Информационно-экономические аспекты стандартизации и технического регулирования. 2026. № 1(88). С. 49–54.

ВВЕДЕНИЕ

Интенсивная цифровая трансформация всех сфер общественной жизни и государственного управления детерминирует возникновение новых вызовов в области обеспечения правопорядка и общественной безопасности. В этих условиях деятельность органов внутренних дел (ОВД) Российской Федерации не только претерпевает значительные изменения, но и становится все более зависимой от надежности и защищенности информационно-телекоммуникационных систем [1]. Обработка значительных массивов оперативно-служебной, розыскной информации и персональных данных, функционирование в составе единой информационной инфраструктуры государственных органов предъявляют исключительно высокие требования к уровню профессиональной компетентности сотрудников в сфере информационной безопасности (ИБ) [2]. Недостаточная подготовленность личного состава к противодействию современным киберугрозам способна привести к системным сбоям, утечке конфиденциальной информации и, как следствие, к снижению эффективности выполнения ключевых задач МВД России [3].

Стратегическая важность данного направления закреплена на высшем государственном уровне, в том числе в таких документах, как Стратегия национальной безопасности Российской Федерации и Доктрина информационной безопасности [4]. Реализация государственной политики в области обеспечения ИБ невозможна без наличия в силовых структурах высококвалифицированных кадров, обладающих не только глубокими теоретическими знаниями, но и сформированными практическими навыками защиты информации в условиях реальных оперативно-служебных задач^{1,2}. Однако существующая система ведомственного об-

Keywords: professional competence, information security, internal affairs bodies, digital transformation, protection of official information, cyber threats, personnel training.

For citation: Nechay A.A., Alekseeva O.V., Gonchar A.A. Formation Of Professional Competence In The Field Of Information Security For Employees Of The Internal Affairs Bodies Of Russia Under Conditions Of Digitalization. Information and Economic Aspects of Standardization and Technical Regulation. 2026; 1(88): 49–54. (In Russ.).

разования сталкивается с рядом вызовов, среди которых – стремительное обновление видов и методов компьютерных атак, недостаточная интеграция практико-ориентированных компонентов в учебные программы, а также необходимость формирования особой культуры информационной безопасности, учитывающей специфику служебной деятельности [5].

Анализ современных исследований, таких как работы Шугаль Н. Б., Бондаренко Н. В., Варламовой Т. А., посвященных цифровой среде [6], позволяет утверждать, что ее развитие неразрывно связано с рисками, многократно возрастающими в контексте правоохранительной деятельности. Исследования Салихова Б. В. и Салихова И. С. подтверждают, что создание защищенной среды является критическим фактором эффективности любой организации, что в полной мере относится и к ОВД [7]. Вместе с тем в научной литературе наблюдается дефицит комплексных исследований, направленных именно на построение целостной модели формирования ИБ-компетенций у сотрудников полиции, с учетом всей совокупности правовых, организационных и технических аспектов их будущей профессии [8].

Актуальность настоящего исследования обусловлена настоятельной необходимостью преодоления разрыва между традиционными подходами к профессиональной подготовке сотрудников ОВД и реальными требованиями, диктуемыми цифровой эпохой [9]. Цель исследования заключается в разработке теоретически обоснованных и практико-ориентированных рекомендаций по совершенствованию процесса формирования профессиональной компетентности в области информационной безопасности у курсантов и сотрудников органов внутренних дел [10]. Практическая значимость исследования заключается в возможности прямого применения его результатов для модернизации учебных планов, разработки специализированных тренажеров и методических материалов, что в конечном итоге будет способствовать усилению защищенности информационного периметра МВД России и повышению эффективности выполнения им своих функций.

¹ Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

² Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

МЕТОДОЛОГИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ

Решение поставленной исследовательской задачи – разработки научно обоснованной модели формирования профессиональной компетентности в области информационной безопасности у сотрудников органов внутренних дел – потребовало применения системы взаимодополняющих методологических подходов. Комплексный характер исследования определил необходимость сочетания теоретического анализа с эмпирической проверкой выдвинутых предположений, что обеспечило достоверность и валидность полученных результатов. Методологическим основанием работы стал системный подход, позволивший рассмотреть процесс профессиональной подготовки как целостный феномен, функционирующий в контексте оперативно-служебной деятельности. Такой ракурс исследования дал возможность учесть влияние внешних факторов, включая постоянную эволюцию киберугроз и динамику законодательного регулирования.

Первоначальный этап исследования базировался на теоретико-методологическом анализе, в рамках которого было проведено комплексное изучение научных публикаций, нормативных правовых актов и ведомственных документов МВД России, который позволил не только выявить современное состояние разрабатываемой проблемы, но и сформировать понятийный аппарат исследования, а также идентифицировать системные противоречия между практическими требованиями к компетенциям сотрудников и реальным содержанием образовательных программ. Для выявления лучших практик и существующих дефицитов в системе ведомственной подготовки был задействован сравнительно-сопоставительный метод. Его применение позволило осуществить детальное сопоставление учебных планов и программ профильных образовательных организаций МВД России, а также проанализировать релевантный зарубежный опыт подготовки сотрудников правоохранительных органов к противодействию современным киберугрозам.

Важное место в исследовании занял метод экспертной оценки, направленный на верификацию теоретических выводов и получение репрезентативных данных о практических аспектах проблемы. В этих целях был организован опрос в формате структурированного интервью с пятнадцатью экспертами, среди которых были действующие сотрудники оперативных и следственных подразделений МВД России, преподаватели ведомственных вузов и специалисты по защите информации из ИТ-подразделений территориальных органов МВД России. Анкетирование экспертов было ориентировано на оценку актуальности выделенных компетенций, выявление типичных проблем в практической деятельности и сбор конструктивных предложений по совершенствованию системы обучения.

Разработанная в ходе исследования структурно-функциональная модель формирования ИБ-компетентности стала результатом применения метода моделирования. Для апробации ключевых элементов данной модели использовался метод ситуационного анализа, в рамках которого курсантам предлагалось разрешить смоделированные проблемные ситуации, связанные с утечкой данных, фишинг-атаками и нарушением регламентов работы со служебной информацией. Обработка полученных эмпирических данных осуществлялась с привлечением статистических методов, что обеспечило наглядность и объективность выводов исследования. Интеграция перечисленных методов позволила сохранить комплексный характер работы, успешно сочетая теоретический анализ с решением прикладных задач, направленных на совершенствование кадровой политики МВД России в условиях цифровой трансформации.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Проведенное исследование позволило получить комплекс данных, характеризующих современное состояние процесса формирования профессиональной компетентности в области информационной безопасности у сотрудников органов внутренних дел. Центральным результатом работы стала разработка структурно-функциональной модели, представленной на рисунке, интегрирующей нормативные, содержательные, процессуальные и оценочно-результативные компоненты.



Структурно-функциональная модель формирования профессиональной компетентности в области информационной безопасности у сотрудников ОВД

Разработанная модель включает следующие структурные блоки:

Целевой блок. Определяет задачу и стратегические цели процесса формирования компетентности. Задача модели заключается в обеспечении устойчивой готовности сотрудников ОВД к противодействию современным киберугрозам. В рамках данной задачи реализуются стратегические цели: формирование системных знаний в области нормативно-правового регулирования ИБ, развитие практических навыков идентификации и нейтрализации кибератак, а также воспитание профессиональной культуры безопасного обращения со служебной информацией.

Содержательный блок модели структурирован вокруг трех ключевых модулей. Нормативно-правовой модуль охватывает законодательство РФ в области ИБ, ведомственные регламенты и международные стандарты защиты информации. Техничко-технологический модуль включает методы криптографической защиты, средства обнаружения вторжений и протоколы безопасного сетевого взаимодействия. Оперативно-тактический модуль сфокусирован на тактике действий при киберинцидентах, методах расследования киберпреступлений и процедурах обеспечения безопасности оперативно-розыскных мероприятий.

Процессуальный блок реализуется через последовательность этапов. Диагностический этап (1 месяц) включает оценку исходного уровня компетенций и формирование индивидуальных траекторий обучения. Теоретико-методологический этап (2 месяца) посвящен модульному изучению нормативных основ и принципов работы защищенных информационных систем. Практико-ориентированный этап (3 месяца) предполагает работу на специализированных тренажерах, решение ситуационных задач по реальным инцидентам и участие в учебных киберучениях.

Оценочно-результативный блок устанавливает критерии эффективности подготовки: качество выполнения нормативных тестовых заданий (40%), успешность решения практических кейсов (35%) и результаты участия в комплексных учениях (25%). Модель предусматривает три уровня сформированности компетенций: базовый (знание нормативных требований), продвинутый (умение применять стандартные процедуры защиты) и экспертный (способность разрабатывать и реализовывать комплексные меры противодействия угрозам).

Эмпирическая апробация элементов разработанной модели, проводившаяся в течение шести месяцев с участием 127 курсантов ведомственного образовательного учреждения, подтвердила ее эффективность. Сравнительный анализ с контрольной группой (115 курсантов) показал статистически значимое превышение показателей экспериментальной группы по параметрам практического применения знаний.

При решении ситуационных задач, моделирующих реальные инциденты информационной безопасности, курсанты экспериментальной группы демонстрировали на 42% более высокие результаты в области идентификации фишинг-атак и на 37% – в применении регламентов защиты конфиденциальной информации.

Важным аспектом исследования стало выявление зависимости между методами обучения и уровнем формирования профессиональных компетенций. Применение методов обучения, основанных на анализе реальных или смоделированных ситуаций (кейсов) на основе реальных инцидентов информационной безопасности, зафиксированных в территориальных органах МВД, позволило повысить уровень осознанного применения процедур защиты информации на 56% по сравнению с традиционными лекционными формами обучения. Наблюдение за практическими занятиями показало, что курсанты, участвовавшие в апробации, в 3,2 раза реже допускали нарушения регламентов работы со служебной информацией при выполнении комплексных заданий.

Особый интерес представляют данные, полученные в ходе экспертной оценки. Анализ результатов структурированного интервью с 15 экспертами выявил согласованность относительно необходимости формирования не только технических навыков, но и культуры личной ответственности за сохранность служебной информации. 93% экспертов отметили, что существующая система подготовки недостаточно ориентирована на профилактику внутренних угроз информационной безопасности, связанных с человеческим фактором.

Реализация предложенной модели потребовала разработки специализированного учебно-методического комплекса, включающего модули ситуационного моделирования, лабораторные практикумы по выявлению уязвимостей и методики проведения учебных тревог по отработке действий при инцидентах, связанных с преступлениями в сфере компьютерной информации. Апробация данного комплекса показала его эффективность в формировании устойчивых практических навыков: после прохождения полного курса подготовки 89% курсантов демонстрировали стабильно высокие результаты при решении комплексных задач по защите информации.

Статистическая обработка данных подтвердила гипотезу о взаимосвязи между использованием активных методов обучения и уровнем сформированности профессиональных компетенций. Корреляционный анализ показал наличие сильной прямой связи ($r = 0,82$) между количеством практических занятий с использованием реальных кейсов и успешностью выполнения итоговых комплексных заданий, а дисперсионный анализ продемонстрировал статистически значимые различия ($p < 0,01$) между показателями экспериментальной и контрольной групп по всем оцениваемым параметрам.

ВЫВОДЫ

Проведенное исследование позволило сформулировать ряд принципиальных положений, имеющих определяющее значение для совершенствования системы подготовки сотрудников ОВД в области информационной безопасности. Разработанная структурно-функциональная модель продемонстрировала свою эффективность как инструмент преодоления разрыва между теоретической подготовкой и практическими требованиями оперативно-служебной деятельности. Экспериментально доказано, что интеграция нормативных, содержательных и оценочных компонентов обеспечивает формирование устойчивых профессиональных компетенций, позволяющих адекватно реагировать на современные киберугрозы.

Эмпирические данные убедительно свидетельствуют о качественном превосходстве практико-ориентированного подхода к обучению. Значительное улучшение показателей идентификации фишинг-атак и применения регламентов защиты информации в экспериментальной группе подтверждает необходимость пересмотра существующего соотношения теоретической и практической подготовки. Особую значимость приобретает использование ситуационных задач на основе реальных инцидентов, что способствует развитию оперативного мышления и формированию навыков принятия решений в условиях, максимально приближенных к реальной оперативной обстановке.

Важнейшим результатом исследования стало осознание необходимости формирования культуры личной ответственности за обеспечение информационной безопасности. Экспертная оценка показала, что технические меры защиты недостаточны без развития у сотрудников осознанного отношения к работе с конфиденциальной информацией. Это обуславливает потребность во внедрении специальных психолого-педагогических методик, направленных

на формирование внутренней мотивации к соблюдению установленных регламентов и процедур.

Статистически значимые различия между экспериментальной и контрольной группами, а также выявленная сильная корреляционная связь между объемом практической подготовки и уровнем сформированности компетенций указывают на перспективность дальнейшего развития предложенного подхода. Разработанный учебно-методический комплекс может служить основой для создания единых стандартов подготовки различных категорий сотрудников ОВД с учетом их специализации и должностных обязанностей.

В контексте цифровой трансформации правоохранительной деятельности особую актуальность приобретает непрерывность процесса формирования компетентности в области информационной безопасности. Полученные результаты свидетельствуют о необходимости создания системы постоянного совершенствования профессиональных навыков, адаптированной к быстро меняющемуся ландшафту киберугроз, что предполагает разработку механизмов регулярного обновления учебных материалов и внедрения передовых методов практической подготовки.

Перспективы дальнейших исследований видятся в углубленном изучении возможностей дифференцированного подхода к подготовке различных категорий сотрудников, а также в разработке специализированных тренажерных комплексов, моделирующих отраслевые особенности кибератак и преступлений в области компьютерной информации. Длительный мониторинг эффективности предложенной модели в реальных условиях оперативно-служебной деятельности позволит оптимизировать процесс формирования профессиональной компетентности и обеспечить необходимый уровень защищенности информационного пространства МВД России.

Список литературы

1. Богачева М.В. Об эволюционировании информационного обеспечения органов внутренних дел в информационную деятельность полиции // Закон и право. 2025. № 6. С. 55–60. – DOI 10.24412/2073-3313-2025-6-55-60.
2. Нечай А. А. Особенности подготовки специалистов для расследования преступлений в сфере компьютерной информации / А.А. Нечай, А.В. Ничагина // Вестник Санкт-Петербургского университета МВД России. 2025. № 4(108). С. 251–261.
3. Федорович В.Ю. Криминалистические технологии и большие данные в процессе подготовки специалистов по противодействию киберугрозам / В.Ю. Федорович, В.А. Минаев // Охрана, безопасность, связь. 2024. № 9–3. С. 206–216.
4. Фролов Р.Н., Дудченко А.В., Колкарева И.Н. Актуальные проблемы стандартизации требований к верификации личности пользователя в сети при организации дистанционного обучения // Информационно-экономические

References

1. Bogacheva M.V. (2025) Ob evolyutsionirovaniy informatsionnogo obespecheniya organov vnutrennikh del v informatsionnuyu deyatel'nost' politzii [On the evolution of information support of internal affairs bodies into the information activities of the police] // Zakon i pravo [Law and Right]. № 6. P. 55–60. DOI 10.24412/2073-3313-2025-6-55-60. (In Russ.).
2. Nechay A.A. (2025) Osobennosti podgotovki spetsialistov dlya rassledovaniya prestupleniy v sfere komp'yuternoy informatsii [Features of training specialists for investigating crimes in the field of computer information] / A.A. Nechay, A.V. Nichagina // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii [Bulletin of the Saint Petersburg University of the Ministry of Internal Affairs of Russia]. № 4(108). P. 251–261. (In Russ.).
3. Fedorovich, V.Yu. (2024) Kriminalisticheskiye tekhnologii i bol'shiye dannye v protsessе podgotovki spetsialistov po protivodeystviyu kiberugrozam [Forensic technologies and big data in the process of training specialists to counter cy-

- аспекты стандартизации и технического регулирования. 2020. № 2 (54). С. 65–71.
5. Нечай А.А. Формирование профессиональной компетентности будущих сотрудников органов внутренних дел в области информационной безопасности на основе структурно-функциональной модели / А.А. Нечай, А.В. Ничагина // Вестник Красноярского государственного педагогического университета им. В.П. Астафьева (Вестник КГПУ). 2025. № 4(74). С. 90–98.
 6. Цифровая среда в образовательных организациях различных уровней: Аналитический доклад / Н.Б. Шугаль, Н.В. Бондаренко, Т.А. Варламова [и др.]. – М.: Национальный исследовательский университет «Высшая школа экономики», 2023. 164 с. – (Мониторинг экономики образования). – DOI 10.17323/978-5-7598-2745-0.
 7. Салихов Б.В. Политическая экономика цивилизационной безопасности в условиях нарастания сложности / Б.В. Салихов, И.С. Салихова. – Москва: Московский университет им. С.Ю. Витте, 2024. 220 с. – ISBN 978-5-9580-0747-9.
 8. Язов Ю.К., Авсентьев А.О. Пути построения многоагентной системы защиты информации от утечки по техническим каналам // Вопросы кибербезопасности. 2022. № 5(51). С. 2–13. – DOI 10.21681/2311-3456-2022-5-2-13.
 9. Карачаев А.Р. Особенности выявления психологических характеристик профессиональной мотивации при профессиональной подготовке сотрудников ОВД // Образование и право. 2022. № 4. С. 337–339. – DOI 10.24412/2076-1503-2022-4-337-339.
 10. Нечай А.А. Цифровая трансформация образования с приоритетом на информационную безопасность // Образование как фактор развития интеллектуально-нравственного потенциала личности и современного общества: Материалы XIV Международной научной конференции, Санкт-Петербург, 8 ноября 2024 года. Санкт-Петербург: Ленинградский государственный университет им. А.С. Пушкина, 2025. С. 29–33.
 - ber threats] / V.Yu. Fedorovich, V.A. Minaev // Okhrana, bezopasnost', svyaz' [Security, Safety, Communication]. № 9-3. P. 206–216. (In Russ.).
 4. Frolov R.N., Dudchenko A.V., Kolkareva I.N. (2020) Aktual'nyye problemy standartizatsii trebovaniy k verifikatsii lichnosti pol'zovatelya v seti pri organizatsii distantsionnogo obucheniya [Current problems of standardizing requirements for user identity verification on the network when organizing distance learning] // Informatsionno-ekonomicheskiye aspekty standartizatsii i tekhnicheskogo regulirovaniya [Information and economic aspects of standardization and technical regulation]. № 2 (54). P. 65–71. (In Russ.).
 5. Nechay, A.A. (2025) Formirovaniye professional'noy kompetentnosti budushchikh sotrudnikov organov vnutrennikh del v oblasti informatsionnoy bezopasnosti na osnove strukturno-funktional'noy modeli [Formation of professional competence of future internal affairs officers in the field of information security based on a structural-functional model] / A.A. Nechay, A.V. Nichagina // Vestnik Krasnoyarskogo gosudarstvennogo pedagogicheskogo universiteta im. V.P. Astaf'yeva (Vestnik KGPU) [Bulletin of the Krasnoyarsk State Pedagogical University named after V.P. Astafiev]. № 4(74). P. 90–98. (In Russ.).
 6. Tsifrovaya sreda v obrazovatel'nykh organizatsiyakh razlichnykh urovney: Analiticheskiy doklad [Digital environment in educational organizations of various levels: Analytical report] / N.B. Shugal', N.V. Bondarenko, T.A. Varlamova [i dr.]. – Moskva: Natsional'nyy issledovatel'skiy universitet «Vysshaya shkola ekonomiki», 2023. 164 p. (Monitoring ekonomiki obrazovaniya [Monitoring of the economics of education]). – DOI 10.17323/978-5-7598-2745-0. (In Russ.).
 7. Salikhov, B.V. (2024). Politicheskaya ekonomiya tsivilizatsionnoy bezopasnosti v usloviyakh narastaniya slozhnosti [Political economy of civilizational security in the context of increasing complexity] / B.V. Salikhov, I.S. Salikhova. – Moskva: Moskovskiy universitet im. S.Yu. Vitte, 2024. 220 p. – ISBN 978-5-9580-0747-9. (In Russ.).
 8. Yazov Yu.K., Avsent'ev A.O. (2022) Puti postroeniya mnogoagentnoy sistemy zashchity informatsii ot utechki po tekhnicheskim kanalim [Ways to build a multi-agent system for protecting information from leakage through technical channels] // Voprosy kiberbezopasnosti [Cybersecurity Issues]. № 5(51). P. 2–13. – DOI 10.21681/2311-3456-2022-5-2-13. (In Russ.).
 9. Karachayev, A.R. (2022). Osobennosti vyyavleniya psikhologicheskikh kharakteristik professional'noy motivatsii pri professional'noy podgotovke sotrudnikov OVD [Features of identifying psychological characteristics of professional motivation during the vocational training of internal affairs officers] / A.R. Karachayev // Obrazovaniye i pravo [Education and Law]. № 4. P. 337–339. DOI 10.24412/2076-1503-2022-4-337-339. (In Russ.).
 10. Nechay, A.A. (2025). Tsifrovaya transformatsiya obrazovaniya s prioriteto na informatsionnyu bezopasnost' [Digital transformation of education with a priority on information security] / A.A. Nechay // Obrazovaniye kak faktor razvitiya intellektual'no-nravstvennogo potentsiala lichnosti i sovremennogo obshchestva: Materialy XIV Mezhdunarodnoy nauchnoy konferentsii, Sankt-Peterburg, 08 noyabrya 2024 goda [Education as a factor in the development of the intellectual and moral potential of the individual and modern society: Proceedings of the XIV International Scientific Conference, St. Petersburg, November 08, 2024]. – Sankt-Peterburg: Leningradskiy gosudarstvennyy universitet im. A.S. Pushkina, P. 29–33. (In Russ.).