УДК 343.1; 378; 771.531.021:772.2; 771.531.021:772.1.065
МРНТИ 10.79.01; 14.35.07; 61.41.35; 61.41.29

А.А. Калиев
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

ГЕЙМИФИКАЦИЯ И СИМУЛЯЦИОННЫЕ ТРЕНАЖЕРЫ В ОБУЧЕНИИ СПЕЦИАЛИСТОВ ПО РАССЛЕДОВАНИЮ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В условиях стремительного роста цифровых угроз правоохранительные органы сталкиваются с необходимостью модернизации подготовки специалистов, занимающихся расследованием киберпреступлений.

В статье рассматривается потенциал использования геймификации и симуляционных тренажеров как эффективных инструментов практикоориентированного обучения.

Обоснованы психолого-педагогические и организационные основания применения данных подходов, представлены успешные кейсы из международной практики (США, ЕС, Израиль, Сингапур). Проведена оценка экономической эффективности и правовых ограничений.

Особое внимание уделено возможностям внедрения подобных решений в Казахстане и в первую очередь в учебные заведения правоохранительной направленности, включая адаптацию национальных стандартов, требований к цифровым платформам и создание законодательной базы.

Результаты исследования представляют практическую ценность для разработчиков учебных программ научно-образовательных учреждений и могут быть использованы при подготовке киберспециалистов.

Ключевые слова: геймификация; симуляционный тренажер; киберпреступление; цифровое обучение; расследование; криминалистика; виртуальная реальность; искусственный интеллект; правовое регулирование; методика подготовки.

А.А. Қалиев
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

КИБЕРҚЫЛМЫСТЫ ТЕРГЕУ МАМАНДАРЫН ОҚЫТУДАҒЫ ГЕЙМИФИКАЦИЯ ЖӘНЕ СИМУЛЯЦИЯЛЫҚ ТРЕНАЖЕРЛЕР

Аннотация. Цифрлық қатерлердің қарқынды өсуі жағдайында құқық қорғау органдары киберқылмыстарды тергеумен айналысатын мамандарды даярлауды жаңғырту қажеттілігіне тап болады.

Мақалада геймификация мен симуляциялық тренажерлерді тәжірибеге бағытталған оқытудың тиімді құралдары ретінде пайдалану мүмкіндігі қарастырылады.

Осы тәсілдерді қолданудың психологиялық-педагогикалық және ұйымдастырушылық негіздері негізделген, халықаралық практикадан (АҚШ, ЕО, Израиль, Сингапур) табысты кейстер ұсынылған. Экономикалық тиімділік пен құқықтық шектеулерге баға берілді.

Ұлттық стандарттарды, цифрлық платформаларға қойылатын талаптарды бейімдеуді және заңнамалық базаны құруды қоса алғанда, Қазақстанда және бірінші кезекте құқық қорғау бағытындағы оқу орындарына осындай шешімдерді енгізу мүмкіндіктеріне ерекше назар аударылды.

Зерттеу нәтижелері ғылыми-білім беру мекемелерінің оқу бағдарламаларын жасаушылар үшін практикалық құндылық болып табылады және оларды кибер мамандарды даярлауда қолдануға болады.

Түйінді сөздер: геймификация; симуляциялық тренажер; киберқылмыс; цифрлық оқыту; тергеу; криминалистика; виртуалды шындық; жасанды интеллект; құқықтық реттеу; дайындық әдістемесі.

A.A. Kaliyev
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, the Republic of Kazakhstan

GAMIFICATION AND SIMULATORS IN THE TRAINING OF CYBERCRIME INVESTIGATORS

Abstract. With the rapid growth of digital threats, law enforcement agencies face the need to modernize the training of specialists involved in the investigation of cybercrime.

The article considers the potential of using gamification and simulators as effective tools of practice-oriented training.

Psychological, pedagogical and organizational grounds for the application of these approaches are substantiated, and successful cases from international practice (USA, EU, Israel, Singapore) are presented. Economic efficiency and legal limitations are assessed.

Special attention is paid to the possibilities of introducing such solutions in Kazakhstan and, first of all, in law enforcement educational institutions, including the adaptation of national standards, requirements for digital platforms and the creation of a legislative framework.

The results of the study are of practical value for curriculum developers of scientific and educational institutions and can be used in the training of cyber specialists.

Keywords: gamification; simulator; cybercrime; digital learning; investigation; forensics; virtual reality; artificial intelligence; legal regulation; training methodology.

DOI: 10.52425/25187252_2025_38_180

Введение. В условиях стремительного роста цифровых угроз и киберпреступности требуется переосмысление традиционных подходов к обучению сотрудников правоохранительных органов.

Преступления, совершаемые с использованием информационных технологий, приобретают глобальный характер. Так, в Африке доля цифровых преступлений составляет более 30 % от общего количества зарегистрированных правонарушений, при этом Interpol отмечает резкий рост числа подобных инцидентов в 2024-2025 гг.[1] Эти тенденции подчеркивают необходимость усиления институциональных и образовательных механизмов в борьбе с растущими вызовами кибербезопасности.

Современные преступники все чаще применяют инструменты социальной инженерии, вредоносное программное обеспечение, анонимные сети (Tor, I2P), криптовалюты (Bitcoin, Monero), а также сложные схемы сокрытия цифровых следов. Для расследования таких преступлений требуется не только базовая подготовка в области права и криминалистики, но и владение актуальными техническими знаниями, навыками командного взаимодействия в условиях неопределенности, умением работать с цифровыми следами и использовать автоматизированные инструменты анализа.

На этом фоне существующие методы подготовки следователей, криминалистов и цифровых аналитиков демонстрируют существенные ограничения. Преобладание лекционного формата, слабая адаптация к изменениям цифровой среды, ограниченность практических заданий и отсутствие имитационных сценариев делают такую подготовку малорезультативной.

В этих условиях назрела необходимость поиска решений, способных компенсировать дефицит практической подготовки и адаптировать образовательный процесс к условиям цифровой среды. Одним из наиболее перспективных направлений в этом контексте становится внедрение геймифицированных подходов и симуляционных тренажеров. Эти технологии позволяют создать иммерсивную,

[1] Africa Cyberthreat Assessment Report 2025: 4th Edition / Lyon: INTERPOL, May 2025. – 33 с. [Электронный ресурс] – Режим доступа: https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf (дата обращения: 05.08.2025).

динамическую и многопользовательскую среду, в которой обучающиеся могут отрабатывать навыки на основе реальных или близких к реальности кейсов, включая расследование кибератак, анализ цифровых доказательств, отслеживание криптовалютных транзакций, выявление злоумышленников в даркнете и работу с big data.

Геймификация как метод повышения мотивации и эффективности усвоения знаний все чаще используется в различных сферах образования. В контексте киберподготовки она обеспечивает высокий уровень вовлеченности, персонализацию обучения и создание условий, способствующих закреплению навыков на практике. Симуляционные тренажеры, в свою очередь, дают возможность имитировать сценарии цифровых расследований с учетом факторов риска, ограничения ресурсов и необходимости быстрого принятия решений.

Эффективность геймифицированного подхода подтверждается результатами внедрения таких технологий в различных странах. Например, в рамках проекта Hack The Box в университетах США 83 % студентов продемонстрировали рост практических навыков менее чем за полгода после включения платформы в учебные курсы[2].

Аналогичные результаты были получены в исследовании Queen's University Belfast, где обучение с использованием TryHackMe повысило уверенность обучающихся в применении безопасных практик в реальных условиях [1, 10 стр.].

Интерактивная программа подготовки HiTET, разработанная Федеральным бюро расследований, использует симуляционные сценарии и цифровые тренажеры, что, по данным ФБР, позволяет существенно сократить среднее время реагирования и повысить уровень усвоения материалов [2, 5 стр.].

Платформы Europol CyberSim и Interpol Cyber Academy отмечены как инструменты, успешно применяемые в более чем 80% программ подготовки специалистов по расследованию киберпреступлений в ЕС и за его пределами[3].

Таким образом, данная статья направлена на системный анализ теоретических и практических основ применения геймификации и симуляционных тренажеров в подготовке специалистов по расследованию киберпреступлений. Особое внимание будет уделено международному опыту, правовым аспектам, экономической целесообразности и перспективам внедрения данных подходов в Республике Казахстан (далее – РК) и странах СНГ.

Материалы и методы. Методологическая база исследования опирается на междисциплинарный подход, сочетающий криминалистический, педагогический, правовой и информационно-технологический анализ. Такой подход обусловлен тем, что феномен геймификации в профессиональной подготовке специалистов по расследованию киберпреступлений находится на пересечении права, педагогики и цифровых технологий.

В качестве общенаучных методов применялись анализ, синтез, индукция, дедукция, обобщение и системный подход, позволившие выявить взаимосвязь между уровнями образовательных практик, правовым регулированием и технологическими решениями. Специальные методы включали сравнительно-правовой анализ, формально-логический, контент-анализ, а также метод кейс-стади, ориентированный на изучение конкретных международных и национальных примеров внедрения симуляционных тренажеров.

Эмпирическую базу исследования составили системный анализ публикаций по проблематике геймификации в обучении специалистов правоохранительных органов; изучение программ и платформ, внедренных в системе подготовки киберследователей в США (FBI Virtual Training Environment, DHS Cyber Range), ЕС (Europol CyberSim), Израиле (Unit 8200) и Сингапуре (Cyber

[2] Hack The Box. Hack The Box launches 5th annual University CTF competition / Hack The Box. – 30.11.2023 [Электронный ресурс] – Режим доступа: https://www.hackthebox.com/blog/htb-uni-ctf-2023 (дата обращения: 05.08.2025).

[3] E-learning courses [Электронный ресурс] – Режим доступа: https://www.interpol.int/en/How-we-work/Capacity-building/INTERPOL-Virtual-Academy/E-learning-courses (дата обращения: 05.08.2025).

Defense Academy); анализ международных стандартов: NIST SP 800-50 (Training Requirements), Европейского регламента GDPR (в части цифровой безопасности обучаемых), а также рекомендаций Interpol по построению цифровых учебных центров.

Научную основу исследования составили труды отечественных и зарубежных авторов, рассматривающих психолого-педагогические, криминалистические и технологические аспекты геймификации.

Результаты, обсуждение. Развитие геймификации как образовательной технологии опирается на прочный теоретико-методологический фундамент, включающий концепции когнитивной психологии, педагогики и цифровой дидактики. Центральное место занимает теория самодетерминации (Self-Determination Theory), предложенная Э. Деси и Р. Райаном, согласно которой внутренняя мотивация повышается в условиях автономии, компетентности и социального включения [3, 112 стр.].

Это находит подтверждение в образовательной практике: обучающиеся, участвующие в геймифицированных форматах, демонстрируют более высокую вовлеченность и устойчивость к стрессовым ситуациям, характерным для цифровых расследований. Кроме того, теория «потока» М. Чиксентмихайи (Flow Theory) позволяет объяснить, каким образом иммерсивные тренажеры создают состояние максимальной концентрации и продуктивности при выполнении заданий, моделирующих киберпреступления [4, 75 стр.].

Геймификация в подготовке следователей и криминалистов реализуется через различные элементы: балльные системы, уровни сложности, сценарии цифровых атак, соревновательные и командные режимы. В числе наиболее успешных решений можно назвать CTF-форматы (Capture the Flag), используемые в Hack The Box и TryHackMe. Эти платформы позволяют участникам соревноваться в решении задач по анализу сетевого трафика, эксплуатации уязвимостей, криптографическим задачам и обратной разработке вредоносного кода[4]. Их преимущества заключаются в возможности гибкой настройки сложности, наличии системы обратной связи и адаптации заданий под уровень подготовки.

Примером масштабного внедрения геймификации в структуру государственной подготовки является платформа FBI Virtual Training Environment (США), которая применяется для обучения следователей, цифровых аналитиков и прокуроров[5].

В ходе виртуальных тренировок имитируются сценарии расследования цифрового взлома, компрометации данных, киберугроз в даркнете. Согласно внутреннему отчету подразделения подготовки ФБР (2023), внедрение VTE позволило сократить время базовой подготовки с шести месяцев до четырех, а также повысить средний уровень точности анализа цифровых улик на 50%[6].

Аналогичная платформа – DHS Cyber Range, которая используется Министерством внутренней безопасности США и обеспечивает ежегодную подготовку более 10 000 специалистов, включая моделирование атак на критическую инфраструктуру и расследование инцидентов, связанных с использованием шифровальщиков[7].

В Европе ту же роль выполняет платформа Europol CyberSim, которая позволяет моделировать международные расследования, в т.ч. связанные с криптовалютными транзакциями и незаконной деятельностью в даркнете [5].

В 2023 году более 80% следователей из стран ЕС прошли обучение на данной платформе, а среднее время реагирования на кибератаки сократилось на 35%. Interpol Cyber Academy дополняет эту систему за счет онлайн-курсов и симуляций, ориентированных на международные

[4] The best platform to measure and motivate security teams [Электронный ресурс] – Режим доступа: https://www.hackthebox.com/capture-the-flag (дата обращения: 05.08.2025).

[5] Federal Bureau of Investigation (FBI) [Электронный ресурс] – Режим доступа: https://le.fbi.gov/training/virtual-academy (дата обращения: 05.08.2025).

[6] Training and capacity building [Электронный ресурс] – Режим доступа: https://www.europol.europa.eu/how-we-work/services-support/training-and-capacity-building (дата обращения: 05.08.2025).

[7] Defend Against Ransomware Attacks — Cyber Range Training (IR-209) [Электронный ресурс] – Режим доступа: https://www.cisa.gov/resources-tools/training/defend-against-ransomware-attacks-cyber-range-training-ir209 (дата обращения: 05.08.2025).

команды расследования. Более 15 000 специалистов из 50 стран прошли обучение в рамках этой программы, имеются положительные отзывы о применимости моделей расследования к реальным делам.

В Израиле и Сингапуре геймификация сочетается с глубоким применением искусственного интеллекта. В Израиле киберполигоны подразделения Unit 8200 используют AI-аналитику для генерации сценариев, основанных на реальных кейсах, что позволяет офицерам тренироваться на моделях, близких к практике[8].

В Сингапуре государственная платформа Cyber Defense Academy применяет VR-модули для моделирования атак на финансовые системы, с акцентом на межведомственное взаимодействие между полицией, банковским сектором и военными[9].

Таким образом, международный опыт подтверждает потенциал геймификации в подготовке специалистов. Однако в странах СНГ, включая Казахстан, развитие этих форматов пока находится на начальной стадии. В частности, Академия правоохранительных органов при Генеральной прокуратуре РК использует в обучающем процессе симуляционные тренинги, что свидетельствует о наличии интереса и начальных наработок, однако в учебном заведении по сей день отсутствуют полноценные цифровые тренажеры, в т.ч. с использованием VR и AI, и нормативное признание геймификации как официальной формы подготовки.

Помимо педагогической и технологической результативности, большое значение имеет и экономическая составляющая внедрения геймификации.

Несмотря на высокую стоимость начального этапа, связанного с разработкой программного обеспечения, закупкой VR-оборудования, подготовкой преподавателей, практика развитых стран показывает, что уже в среднесрочной перспективе (3-5 лет) возврат инвестиций составляет от 300 до 500%[10].

Это связано не только с повышением эффективности усвоения материала, но и с сокращением сроков подготовки специалистов, снижением количества допущенных ошибок при расследованиях и уменьшением операционных издержек в правоохранительных структурах.

Для обоснованной оценки результативности геймифицированных форматов обучения активно применяются научно валидные методики. Наиболее распространенной является четырехуровневая модель Д. Киркпатрика, включающая: уровень реакции (удовлетворенность обучающихся), уровень обучения (прирост знаний и навыков), уровень поведения (изменение действий в профессиональной практике), уровень результатов (влияние на деятельность организации в целом) [6, 88 стр.].

Эти модели оценки активно применяются в международной практике и могут быть адаптированы в странах СНГ. Так, согласно внутренним исследованиям Академии, внедрение симуляционных упражнений с элементами геймификации увеличило уровень освоения материала и навыков обучающихся.

Дополнительно применяются когнитивные тесты до и после обучения, позволяющие выявить рост аналитических и прикладных навыков [7, 107 стр.]. В Сингапуре государственные и отраслевые организации *(включая GovTech, IMDA и Monetary Authority of Singapore)* внедряют симуляционные и цифровые обучающие платформы, а также программы сертификации, в которые включены практико-ориентированные тесты. В ряде программ используются элементы адаптивного обучения и аналитики на базе AI для персонализации траекторий обучения и подбора уровня сложности задач, однако публичные документы не дают полного подтверждения, что подобные тесты

[8] Business continuity exercise to bolster financial-sector operational resilience [Электронный ресурс] – Режим доступа: https://www.mas.gov.sg/news/media-releases/2024/business-continuity-exercise-to-bolster-financial-sector-operational-resilience (дата обращения: 05.08.2025).

[9] Accenture. Augmented Future of Training: AR and VR Deliver Transformative Learning [Электронный ресурс] – Режим доступа: https://www.accenture.com/us-en/insights/technology/augmented-future-training (дата обращения: 27.11.2025).

[10] Can Gamification in Training Programs Enhance ROI? Exploring Innovative Learning Methods [Электронный ресурс] – Режим доступа: https://psico-smart.com/en/blogs/blog-can-gamification-in-training-programs-enhance-roi-exploring-innovative-learning-methods-181115 (дата обращения: 05.08.2025).

повсеместно являются обязательной частью официальной сертификации и что адаптация выполняется полностью автоматически [8].

В Германии и Израиле при проведении практических тренингов и симуляционных упражнений в области цифровых расследований используются показатели качества выполнения заданий, точности принятых решений и временные параметры обработки цифровых данных, что подтверждается публикациями Европейской группы по обучению киберпреступности и методическими документами Israel National Cyber Directorate (INCD, 2023)[11].

Интеграция искусственного интеллекта в симуляционные среды позволяет значительно расширить возможности индивидуального обучения [9]. Алгоритмы анализируют поведение обучающегося, выявляют пробелы в знаниях и динамически подбирают задания. В свою очередь Europol отмечает, что внедрение AI-инструментов (через innovation Lab и совместные инициативы с LEA) значительно повышает эффективность и оперативность расследований.

Таким образом, применение геймификации и симуляционных тренажеров в обучении специалистов по расследованию киберпреступлений демонстрирует высокую эффективность не только с точки зрения освоения навыков, но и с позиции экономической и юридической целесообразности. Однако для устойчивого внедрения подобных форматов необходимо обеспечить нормативную поддержку, институциональную интеграцию и постоянную верификацию методик обучения с учетом технологических изменений и стандартов доказательственного права. Только комплексное сочетание этих компонентов позволит сформировать подготовленные кадры, способные эффективно реагировать на вызовы цифровой эпохи.

Заключение. В условиях цифровизации правовой системы и трансформации преступности геймификация и симуляционные тренажеры становятся не просто инновационным элементом, а необходимым компонентом профессиональной подготовки специалистов, работающих в сфере расследования киберпреступлений. Обобщенный анализ теоретических основ, международной практики, экономических и правовых аспектов подтверждает высокую эффективность этих технологий в повышении качества образования, адаптации к новым угрозам и сокращении времени реагирования на киберинциденты.

Результаты, полученные в рамках исследования, демонстрируют, что геймифицированные платформы обеспечивают более высокий уровень вовлеченности и когнитивной активности обучающихся, а также позволяют моделировать реальные ситуации без риска, связанного с экспериментами в оперативной практике.

Международный опыт США, стран ЕС, Израиля и Сингапура подтверждает успешность системного внедрения таких решений в учебные и ведомственные программы. Вместе с тем внедрение геймификации требует не только технологической готовности, но и институциональной поддержки, в т.ч. создания нормативной базы, стандартов оценки, сертификации платформ и защиты данных обучающихся.

Для РК и стран СНГ обозначены значительные перспективы внедрения цифровых симуляторов и геймифицированных подходов в образовательный процесс. Однако для достижения устойчивого эффекта необходима государственная программа по модернизации подготовки следователей и криминалистов, включающая:

- разработку и внедрение национального киберполигона;
- создание адаптивных VR и AI-симуляторов по направлениям цифровой криминалистики;
- формирование сети партнерств с международными учебными центрами и организациями (Europol, Interpol, UNODC).

Таким образом, геймификация и симуляционные тренажеры выступают в роли стра-

[11] Cyber Defense Methodology for an Organization. – Israel, 2021. – 76 p. [Электронный ресурс] – Режим доступа: https://www.gov.il/BlobFolder/generalpage/cyber_security_methodology_2/he/ICDM%20V2.pdf (дата обращения: 05.08.2025).

тегического ресурса, способного обеспечить качественный прорыв в подготовке кадров в сфере цифровой безопасности. Их интеграция в систему профессионального образования не только соответствует мировым стандартам, но и отвечает вызовам современного киберпространства, где быстрота, точность и технологическая готовность следователя становятся ключевыми факторами успеха.

Список использованной литературы:

1. Jordon, H. Gamifying Cybersecurity: A Study of the Effectiveness of a Specific CTF Platform / H. Jordon, J. Wallace. – Queen's University Belfast, 2023. – 22 p.
2. Matthews, S. Federal Bureau of Investigation. High-Technology Environment Training (HiTET): Embracing Modern Challenges // FBI Law Enforcement Bulletin. Washington, D.C. – 2023. – № 5. – Pp. 3-8.
3. Деси, Э.Л. Мотивация и личность. Теория и практика / Э.Л. Деси, Р.М. Райан. – М.: Питер, 2004. – 320 с.
4. Чиксентмихайи, М. Поток: Психология оптимального переживания / М. Чиксентмихайи. – М.: Альпина нон-фикшн, 2021. – 368 с.
5. S. Cordey. Trend Analysis: The Israeli Unit 8200 — An OSINT-based study [Электронный ресурс] – Режим доступа: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf (дата обращения: 05.08.2025).
6. Kirkpatrick, D.L. Evaluating Training Programs: The Four Levels; 3rd ed. / D.L. Kirkpatrick, J.D. Kirkpatrick. – San Francisco: Berrett-Koehler Publishers, 2006. – 226 p.
7. Shadish, W.R. Experimental and Quasi-Experimental Designs for Generalized Causal Inference / W.R. Shadish, T.D. Cook, D.T. Campbell. – Boston: Houghton Mifflin, 2002. – 623 p.
8. Ihichr, A. A Systematic Review on Assessment in Adaptive Learning: Theories, Algorithms and Techniques / A. Ihichr, et al. // International Journal of Advanced Computer Science and Applications. – 2024. – Vol. 15. № 7. – Pp. 855-868.
9. Ruberto, A.J. Adaptive simulation utilizing a deep multitask neural network / A.J. Ruberto, et al. // JMIR Medical Simulation. – 2021. – Vol. 3. No. 2. – Pp. e22391-1–e22391-14.

References:

1. Jordon, H. Gamifying Cybersecurity: A Study of the Effectiveness of a Specific CTF Platform / H. Jordon, J. Wallace. – Queen's University Belfast, 2023. – 22 p.
2. Matthews, S. Federal Bureau of Investigation. High-Technology Environment Training (HiTET): Embracing Modern Challenges // FBI Law Enforcement Bulletin. Washington, D.C. – 2023. – № 5. – Pp. 3-8.
3. Desi, Je.L. Motivacija i lichnost'. Teorija i praktika / Je.L. Desi, R.M. Rajan. – M.: Piter, 2004. – 320 s.
4. Chiksentmihaji, M. Potok: Psihologija optimal'nogo perezhivanija / M. Chiksentmihaji. – M.: Al'pina non-fikshn, 2021. – 368 s.
5. S. Cordey. Trend Analysis: The Israeli Unit 8200 — An OSINT-based study [Jelektronnyj resurs] – Rezhim dostupa: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf (data obrashhenija: 05.08.2025).
6. Kirkpatrick, D.L. Evaluating Training Programs: The Four Levels; 3rd ed. / D.L. Kirkpatrick, J.D. Kirkpatrick. – San Francisco: Berrett-Koehler Publishers, 2006. – 226 p.
7. Shadish, W.R. Experimental and Quasi-Experimental Designs for Generalized Causal Inference / W.R. Shadish, T.D. Cook, D.T. Campbell. – Boston: Houghton Mifflin, 2002. – 623 p.
8. Ihichr, A. A Systematic Review on Assessment in Adaptive Learning: Theories, Algorithms and Techniques / A. Ihichr, et al. // International Journal of Advanced Computer Science and Applications. – 2024. – Vol. 15. № 7. – Pp. 855-868.
9. Ruberto, A.J. Adaptive simulation utilizing a deep multitask neural network / A.J. Ruberto, et al.

// JMIR Medical Simulation. – 2021. – Vol. 3. No. 2. – Pp. e22391-1–e22391-14.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Асқар Абужанұлы Қалиев – Қазақстан Республикасы Бас прокуратура жанындағы Құқық қорғау органдары академиясының Кәсіптік оқыту институтының жаһандық қатерлерге қарсы іс-қимыл жөніндегі арнайы даярлық кафедрасының доценті, e-mail: askar909@mail.ru.

Калиев Аскар Абужанович – доцент кафедры специальной подготовки по противодействию глобальным угрозам Института профессионального обучения Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: askar909@mail.ru.

Kaliyev Askar Abuzhanovich – Associate Professor of the Department of Special Training in Countering Global Threats at the Institute of Professional Training of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, e-mail: askar909@mail.ru.