Научная статья
УДК 378

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ КУРСАНТОВ ВОЕННЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ВЫСШЕГО ОБРАЗОВАНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Дмитрий Викторович Гудов[1]✉, Денис Александрович Богданов[2]
[1, 2] Саратовский военный ордена Жукова Краснознаменный институт войск национальной гвардии, Саратов, Россия
[1] gdim@yandex.ru✉
[2] svki.bogdanov@yandex.ru

Аннотация. В сложившихся современных условиях образовательной политики государства и обеспечения ее обороноспособности особое внимание уделяется военному образованию, формированию у будущих офицеров войск национальной гвардии Российской Федерации готовности к решению служебно-боевых задач по своему профессиональному предназначению. Профессиональная подготовка специалистов в области информационной безопасности, а также развитие информационных технологий - характерная черта современного общества. Эти аспекты делают вопрос целенаправленной подготовки квалифицированных кадров в области информационной безопасности особенно актуальным. Требования к специалистам по информационной безопасности в любой структуре достаточно высоки, так как в настоящее время они должны противостоять всевозможным угрозам. Совершенствование подготовки специалистов в области защиты информации следует отнести к приоритетным задачам государства в области защиты информации.

Ключевые слова: информационные технологии, военное образование, защита информации, киберугроза, кибербезопасность

Для цитирования: Гудов Д. В., Богданов Д. А. Использование информационных технологий при подготовке курсантов военных образовательных организаций высшего образования в области защиты информации // Известия Саратовского военного института войск национальной гвардии. 2025. № 3 (20). С. 12–21. URL: https://svkinio.ru/2025/3(20)/Gudov_Bogdanov.pdf.

Original article

USE OF INFORMATION TECHNOLOGIES IN TRAINING CADETS OF THE ALL-RUSSIAN SOCIETY OF MILITARY ENGINEERS IN THE FIELD OF INFORMATION SECURITY

Dmitriy V. Gudov[1]✉, Denis A. Bogdanov[2]
[1, 2] Saratov Military Order of Zhukov Red Banner Institute of the National Guard Troops, Saratov, Russia
[1] gdim@yandex.ru✉
[2] svki.bogdanov@yandex.ru

Abstract. In the current modern conditions of the state's educational policy and ensuring its defense capability, special attention is paid to military education, the formation of readiness in future officers of the troops of the National Guard of the Russian Federation to solve service and combat tasks according to their professional purpose. Professional training of specialists in the field of information security, as well as the development of information technologies, is a characteristic feature of modern society. These aspects make the issue of targeted training of qualified personnel in the field of information security particularly relevant. The requirements for information security specialists in any structure are quite high,

as they must currently resist all sorts of threats. Improving the training of specialists in the field of information security should be considered a priority task for the state in the field of information security.

Keywords: information technology, military education, information protection, cyber threat, cybersecurity

For citation: Gudov D. V., Bogdanov D. A. Use of information technologies in training cadets of the all-Russian society of military engineers in the field of information security. *Izvestija of the Saratov Military Institute of the National Guard Troops*. 2025;(3):12-21. Available from: https://svkinio.ru/2025/3(20)/Gudov_Bogdanov.pdf. (In Russ.).

В условиях актуальных приоритетов государственной образовательной стратегии и стремления к укреплению обороноспособности страны существенно возрастает значимость развития системы военного образования. В центре внимания оказывается формирование у курсантов войск национальной гвардии Российской Федерации (далее – Росгвардии) готовности к решению профессионально-боевых задач, соответствующих современным вызовам и требованиям.

Особую значимость в этом контексте приобретает подготовка специалистов в сфере информационной безопасности. Интенсивное внедрение цифровых решений в различные сферы жизнедеятельности общества и ускоренная трансформация информационно-коммуникационной среды обуславливают необходимость наличия высококвалифицированных кадров, способных эффективно обеспечивать защиту информации. На фоне усложняющихся киберугроз и возрастающих рисков в цифровом пространстве потребность в компетентных специалистах становится стратегически важной.

Современные стандарты профессиональной деятельности в области информационной безопасности предъявляют высокие требования к уровню подготовки специалистов. Они должны быть способны своевременно выявлять потенциальные угрозы, анализировать уязвимости информационных систем и реализовывать комплексные меры защиты. В силу этого актуальность подготовки офицеров в данной области обоснованно рассматривается в качестве одного из ключевых направлений государственной политики в сфере обеспечения информационной безопасности [1].

Современное общество испытывает значительные трансформации под воздействием стремительного развития информационных технологий. Эти изменения охватывают широкий спектр информационных структур и субъектов, осуществляющих сбор, обработку, распространение и использование данных. Массовая цифровизация и внедрение передовых информационных технологий в повседневную жизнь привели к кардинальному изменению характера деятельности в сферах образования, экономики, промышленности, науки и социальной коммуникации.

В условиях растущей зависимости от информации, последняя приобретает статус важнейшего стратегического ресурса, а обеспечение её сохранности — одного из приоритетов как на уровне отдельных организаций, так и в масштабах государства. Систематическое нарастание киберугроз, проявляющихся в формах утечек данных, деструктивных вмешательств и целенаправленных атак на информационные системы, требует выработки эффективных подходов к защите информации.

В связи с этим образовательные учреждения, готовящие специалистов в области информационной безопасности, сталкиваются с задачей адаптации программ подготовки к быстро меняющемуся характеру угроз и технологий. Образовательный процесс должен учитывать как современные вызовы, так и особенности функционирования информационных систем в специфических условиях, включая режимы ограниченного доступа и повышенной секретности. Особенно актуальной становится задача формирования у курсантов Росгвардии готовности к противодействию киберугрозам, поскольку в условиях проведения специальной военной операции ин-

формационная безопасность приобретает критическое значение в обеспечении устойчивости национальной обороны [2].

Анализ научных публикаций свидетельствует о том, что становление системы подготовки специалистов в области информационной безопасности характеризуется определённой историко-структурной динамикой. Этот процесс включает последовательные этапы, каждый из которых отражает смену образовательных приоритетов, технологических решений и организационно-методических подходов. Выделение этапов осуществляется на основе таких факторов, как содержание подготовки, институциональные особенности и характер применяемых педагогических и технических инструментов.

В современных условиях особое значение приобретает подготовка будущих офицеров Росгвардии, ориентированная на развитие устойчивых компетенций, необходимых для выполнения задач в условиях постоянных изменений. Возрастающая сложность служебно-боевых задач, внедрение новых типов вооружения и информационных технологий обуславливают необходимость системного обновления образовательного содержания [3].

Актуальность данной проблемы обусловлена рядом факторов: во-первых, стремительным изменением структуры профессиональной деятельности, появлением новых специальностей и направлений, требующих специфических знаний и навыков; во-вторых, возрастающей потребностью в гибких, многопрофильных специалистах, способных адаптироваться к нестандартным условиям службы; в-третьих, модернизацией материально-технической базы, которая диктует необходимость овладения современными средствами связи, защиты информации и автоматизированными системами управления. Всё это требует комплексного пересмотра подходов к подготовке курсантов, ориентированных на выполнение служебных задач в условиях повышенной ответственности и растущих профессиональных требований.

Современные преобразования в системе высшего военного образования свидетельствуют о переходе к инновационной образовательной модели, ориентированной на формирование не только профессиональных, но и личностных качеств офицеров. В рамках этой парадигмы особое внимание уделяется развитию когнитивных способностей, гибкости мышления, способности к принятию решений в нестандартных условиях, а также формированию профессионально значимых установок и ценностей [4].

Новая модель военной подготовки не отвергает сложившиеся педагогические подходы, а напротив, интегрирует их в обновлённую структуру, адаптированную к современным реалиям. Её ключевые компоненты можно выделить следующим образом:

- активное внедрение современных цифровых и информационно-аналитических систем в учебный процесс, что повышает эффективность усвоения материала и приближает учебные задачи к реальным ситуациям служебной деятельности;

- расширенное использование методов контекстного обучения, позволяющего моделировать профессиональные ситуации, с которыми будущие офицеры могут столкнуться в условиях оперативной обстановки;

- применение научно обоснованных психолого-педагогических подходов в подготовке военнослужащих, в частности, формирование устойчивых педагогических и управленческих компетенций, необходимых для функционирования в военной системе и в роли наставника.

Таким образом, модернизация образовательной парадигмы не ограничивается обновлением технических средств обучения, а охватывает более глубокие аспекты формирования профессиональной идентичности офицера, подчеркивая значимость интеграции информационных технологий, моделирующих методик и педагогической культуры.

Профессиональная подготовка курсантов, ориентированных на службу в подразделениях Росгвардии, представляет собой целостную образовательную систему, направленную на формирование у обучающихся комплекса интегральных компетенций, обеспечивающих готовность к выполнению функциональных обязанностей в условиях оперативно-служебной деятельности [5]. Эта система носит целенаправ-

ленный и многокомпонентный характер, включающий как нормативно-правовые, так и педагогико-технологические основания.

Важнейшими направлениями профессиональной подготовки являются:

1. Формирование компетентностного профиля — развитие универсальных (коммуникативных, организационных), общепрофессиональных (управление информационными потоками, работа с ресурсами) и специализированных (военно-прикладных, технических, в том числе связанных с защитой информации) компетенций.

2. Соблюдение требований ФГОС ВО — обеспечение соответствия образовательного процесса государственным стандартам, предполагающим баланс теоретических знаний и прикладных навыков, особенно в области информационных и вычислительных технологий.

3. Учет квалификационных характеристик — подготовка курсантов к выполнению специфических задач, определяемых регламентом служебной деятельности и требованиями к офицерам подразделений, участвующих в обеспечении информационной безопасности.

4. Личностно-ориентированный компонент — развитие у будущих офицеров способности к профессиональному самоопределению, формирование устойчивых морально-этических установок, стрессоустойчивости и готовности к действию в условиях неопределённости и повышенной ответственности.

Такой подход позволяет сформировать у курсантов не только необходимый объем знаний и умений, но и систему ценностей, соответствующих специфике службы в Росгвардии, где защита информации становится неотъемлемой частью обеспечения государственной безопасности.

Актуальные вызовы в области защиты информации охватывают широкий диапазон направлений — от обеспечения физической безопасности объектов до противодействия высокотехнологичным цифровым атакам. В условиях возрастающей зависимости всех сфер жизнедеятельности от информационных систем значимость кибербезопасности становится определяющей. Специалисты, работающие в этой области, обязаны обладать не только обширными техническими знаниями, но и навыками оперативного реагирования на сложные и быстро эволюционирующие угрозы.

В едином информационном пространстве Росгвардии также фиксируется растущее число уязвимостей, возникающих в результате активного применения информационных технологий в служебной деятельности. С одной стороны, ИТ -решения обеспечивают высокий уровень функциональности и взаимодействия, а с другой — расширяют спектр потенциальных точек для атак. Обеспечение защиты информационных ресурсов в структуре национальной гвардии следует рассматривать как приоритетное направление в рамках реализации стратегии информационной безопасности государства. Эта стратегия предполагает системный подход к защите критически важной инфраструктуры, противодействию кибершпионажу, предотвращению кибератак и другим формам вмешательства. В условиях обострения геополитических угроз особенно возрастает значимость формирования устойчивой архитектуры информационной безопасности, в том числе посредством эффективной подготовки кадров [6].

Решение вышеуказанных задач требует от специалистов по защите информации Росгвардии постоянного мониторинга ситуации в киберпространстве, аналитических способностей и умения проектировать и реализовывать защитные меры. Информационная безопасность перестает быть вспомогательной функцией и превращается в один из ключевых элементов оборонной доктрины наравне с вооружённой и тактической составляющей.

Несмотря на значительное внимание, уделяемое вопросам кибербезопасности, практика демонстрирует наличие комплекса системных проблем, препятствующих эффективной защите информации в структуре войск национальной гвардии. Одной из ключевых трудностей выступает высокая степень зависимости от цифровых решений и информационно-технических систем, которые нередко обладают уязвимостями, доступными как для внешних злоумышленников, так и для внутренних нарушителей [1].

Многообразие потенциальных угроз включает в себя атаки различной направленности: от

банального несанкционированного доступа до сложных сценариев вторжений с использованием методов социальной инженерии, вредоносного программного обеспечения и скрытого мониторинга. Кроме того, внутренняя угроза неосторожных пользователей представляет не меньшую опасность, особенно в условиях ограниченного контроля за поведенческими аспектами внутри организаций.

Для минимизации рисков необходим комплексный подход, охватывающий как технологические меры — установку систем обнаружения и предотвращения вторжений, использование многоуровневой аутентификации, постоянный мониторинг событий безопасности — так и управленческие решения. Последние включают повышение уровня осведомлённости персонала, регулярное проведение специализированных обучающих мероприятий, создание культуры информационной безопасности.

Профессиональная деятельность в области информационной безопасности охватывает широкий спектр функциональных ролей, каждая из которых предъявляет специфические требования к компетентностному профилю специалиста. Задачи в этой сфере варьируются от стратегического анализа угроз и оценки рисков до проектирования защитных систем, оперативного мониторинга и реагирования на инциденты. Такое функциональное разнообразие обуславливает необходимость многоуровневой подготовки, сочетающей техническую грамотность с развитым аналитическим и управленческим мышлением.

Особенности профессиональной подготовки в данной области диктуются не только технологическим прогрессом, но и постоянно меняющейся природой киберугроз. Некоторые аспекты деятельности требуют глубокой технической квалификации — в области криптографии, сетевой безопасности, архитектуры информационных систем, другие предполагают высокую степень социально-коммуникативных умений, включая взаимодействие с персоналом, обучение пользователей и формирование организационной культуры безопасности [7].

Таким образом, эффективная защита информации невозможна без интеграции двух ключевых компонентов: технической компетентности и способности к управлению человеческим фактором. Специалист в данной сфере должен уметь не только выявлять и устранять уязвимости, но и формировать поведенческие модели, минимизирующие вероятность человеческих ошибок, а также участвовать в формировании устойчивых стандартов безопасного поведения в организации.

Современная практика требует от специалистов гибкости и готовности к постоянному профессиональному развитию. Новые угрозы, появляющиеся в цифровом пространстве, обусловлены действиями высокоорганизованных атакующих структур, обладающих значительными ресурсами и доступом к современным технологиям [8]. В таких условиях особенно важно формировать у курсантов способность к постоянному обучению, адаптации к новым условиям и креативному решению задач в рамках обеспечения кибербезопасности.

Военные вузы активно внедряют современные информационные технологии и цифровые инструменты для подготовки специалистов по защите информации. Среди наиболее значимых технологий можно выделить:

- киберполигоны и симуляторы кибератак, которые позволяют моделировать реальные сценарии кибервойн, включая DDoS-атаки, взломы сетевой инфраструктуры и противодействие APT-угрозам;

- виртуальная и дополненная реальность (VR/AR) применяются для создания интерактивных тренажеров, где курсанты отрабатывают действия в виртуальных командных центрах или при защите критической инфраструктуры;

- Big Data и искусственный интеллект используются для анализа паттернов кибератак и автоматизированного обучения систем обнаружения вторжений;

- дистанционные образовательные платформы: онлайн-курсы (MOOC), вебинары и облачные лаборатории (например, Cyber Range), позволяют организовать гибкое обучение, включая международные совместные учения.

Однако, наряду с техническими мерами и аналитическими подходами, не менее важной задачей является формирование устойчивой

этической и культурной основы профессиональной деятельности в сфере информационной безопасности. Речь идёт о выработке профессиональных норм поведения, осознании социальной значимости своей деятельности и соблюдении стандартов, направленных на минимизацию угроз как внешнего, так и внутреннего происхождения.

Поэтому одним из направлений подготовки курсантов Росгвардии становится формирование ценностных ориентиров, соответствующих требованиям информационной этики. Это включает развитие личной ответственности, правовой грамотности, способности действовать в рамках нормативной базы и понимать последствия своих решений в киберпространстве. Только при сочетании профессиональной подготовки с этико-правовыми установками возможно создание кадров, способных не просто выполнять технические задачи, но и выступать носителями культуры безопасности в государственном масштабе.

Образовательные программы должны учитывать специфику глобального информационного противоборства, выходящего за рамки национальных границ. Современные вызовы в области кибербезопасности всё чаще носят трансграничный характер, что требует от обучающихся не только владения отечественными технологиями, но и понимания международных правовых норм, стратегий противодействия угрозам, а также способности анализировать глобальные тенденции.

В условиях информационного давления на Россию со стороны иностранных структур и организаций особое значение приобретает формирование цифрового суверенитета. Это понятие охватывает способность государства самостоятельно контролировать критические цифровые ресурсы, разрабатывать и применять отечественные программно-аппаратные решения, а также обеспечивать независимость от внешних поставщиков и платформ.

Для достижения этих целей необходимо не только активное развитие собственных технологических решений, но и подготовка специалистов нового типа — обладающих системным мышлением, высоким уровнем информационной грамотности, способностью к принятию решений в условиях неопределённости. Одним из приоритетов становится формирование эффективных каналов взаимодействия между государственными структурами, образовательными учреждениями и частным сектором для оперативного обмена данными и совместного реагирования на киберугрозы.

В этом контексте инвестиции в качественное военное образование и развитие национальной школы кибербезопасности следует рассматривать не просто как подготовку кадрового резерва, но и как стратегический вклад в укрепление информационного суверенитета и оборонного потенциала государства.

В условиях проведения специальной военной операции информационная безопасность приобретает первостепенное значение как элемент стратегического управления и оперативной устойчивости. Киберпространство становится полноценным театром противоборства, в котором ведутся активные наступательные и оборонительные действия, направленные как на нарушение функционирования критической инфраструктуры, так и на подрыв морально-психологической устойчивости личного состава и гражданского населения.

В таких обстоятельствах подготовка специалистов, способных эффективно противодействовать как классическим, так и гибридным киберугрозам, становится неотъемлемым компонентом оборонного потенциала государства. Речь идёт о способности защищать военные коммуникационные каналы, обеспечивать устойчивость систем связи, предотвращать утечки критически важной информации и оперативно нейтрализовывать последствия цифровых атак [9].

Система подготовки будущих офицеров Росгвардии в области информационной безопасности требует комплексного и многопланового подхода, ориентированного как на теоретическое, так и на практико-ориентированное обучение. Одним из ключевых факторов, определяющих эффективность этой подготовки, выступает широкое и целенаправленное использование информационных технологий. Именно они создают условия для моделирования реаль-

ных киберугроз, реализации учебных симуляций, анализа инцидентов и отработки алгоритмов реагирования [10, 11].

Информационные технологии обеспечивают не только доступ к специализированным знаниям, но и формируют цифровую среду, в которой обучающиеся приобретают навыки работы с современными средствами защиты, системами мониторинга, автоматизированными платформами анализа и технического контроля. Включение информационных технологий в образовательный процесс способствует формированию профессиональной гибкости и способности к адаптации в условиях быстроменяющейся цифровой реальности.

В условиях проведения специальной военной операции и обострения киберпротивостояния роль подготовленных специалистов в сфере защиты информации возрастает многократно. Только системный подход, включающий постоянное обновление содержания подготовки, применение современных образовательных технологий и развитие сотрудничества с индустрией, позволит сформировать кадры, способные обеспечить надёжную защиту информационных ресурсов. Поддержка таких образовательных инициатив является стратегическим вкладом в укрепление национальной безопасности и цифрового суверенитета Российской Федерации.

Список источников

1. Арутюнов, В. В. Современные проблемы и задачи обеспечения информационной безопасности // Вестник Московского финансово-юридического университета МФЮА: науч. журн. 2014. № 3. С. 140–146. ISSN 2224-669X (print). Электрон. версия. URL: https://elibrary.ru/wawktv (дата обращения: 15.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

2. Якушкин, В. П., Богданов, Д. А. Методика изучения основ информационной безопасности в военных образовательных организациях высшего образования войск национальной гвардии Российской Федерации // Информационные технологии и информационная безопасность в профессиональной деятельности: сб. науч. ст. IV межвуз. науч.-практ. конференции с междун. участием (г. Новосибирск, 5 февраля 2025 г.). Новосибирск: Новосибирский воен. ин-т им. генерала армии И. К. Яковлева войск национальной гвардии, 2025. С. 136–141.

3. Луконин, А. В., Нешко, А. Н. Роль информационных технологий в военно-профессиональной подготовке офицеров войск национальной гвардии Российской Федерации // Войска национальной гвардии Российской Федерации: прошлое и настоящее: сб. тр. межвуз. науч.-практ. конференции (к 210-летию образования войск правопорядка и 5-летнему юбилею создания Росгвардии) (г. Саратов, 7 апреля 2021 г.) / под ред. С. В. Бойко. Саратов: Саратовский воен.ордена Жукова Краснознаменный ин-т войск национальной гвардии, 2021. С. 315–325. Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=45750522 (дата обращения: 12.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

4. Журкин, В. В. Особенности формирования ценностных ориентаций курсантов военных вузов войск национальной гвардии Российской Федерации // Социологические знания в контексте актуальных проблем развития социальных общностей и институтов: сб. науч. ст. II Всерос. науч.-практ. конференции (г. Саратов, 29 ноября 2024 г.) / под ред. А. М. Пихтелёва. Саратов: Саратовский воен. ордена Жукова Краснознаменный ин-т войск национальной гвардии, 2024. С. 23–30. Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=80310703 (дата обращения: 10.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

5. Нешко, А. Н., Луконин, А. В., Гудов, Д. В. Роль и место дисциплины «Информатика и информационные технологии в профессиональной деятельности» в системе высшего образования войск национальной гвардии Российской Федерации // Известия Саратовского военного института войск

национальной гвардии: науч. журн. 2020. № 1 (1). С. 31–35. ISSN 2949-5245 (online). URL: https://svkinio.ru/2020/1(1)/Shchukin.pdf (дата обращения: 10.06.2025).

6. Богданов, Д. А. Основные характеристики профессиональной подготовки будущих офицеров подразделений информационных технологий к использованию средств защиты информации // Академический вестник войск национальной гвардии Российской Федерации: науч. журн. 2022. № 2. С. 47–52. ISSN 2658-4336 (print). Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=49348729 (дата обращения: 15.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

7. Логинов, Е. Л. Проблема противодействия информационным атакам на системы критической инфраструктуры России // Вестник Московского университета МВД России: науч. журн. 2013. № 4. С. 201–205. ISSN 2073-0454 (print). ISSN 2782-5698 (online). Электрон. версия. URL: https://www.elibrary.ru/item.asp?edn=qiskkr (дата обращения: 15.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

8. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: Издательский дом Высшей школы экономики, 2015. 574 с. Электрон. версия печ. изд. URL: https://www.elibrary.ru/item.asp?edn=qxtzdq (дата обращения: 13.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

9. Матвиенок, Д. В. Информационный обмен и информационные заимствования как условие развития общества // Культурная жизнь Юга России: науч. журн. 2008. № 2 (27). С. 42–44. ISSN 2070-075X (print). Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=12880029 (дата обращения: 10.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

10. Жук, Е. И. Концептуальные основы информационной безопасности // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. 2010. № 4. С. 7–44. ISSN 1994-0408 (online). Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=14571457 (дата обращения: 11.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

11. Капустин, Ф. А. Информационная безопасность и защита информации в современном обществе // Актуальные проблемы авиации и космонавтики: науч. журн. 2016. Т. 2. № 12. С. 56–58. Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=28146273 (дата обращения: 11.06.2025). Доступна на сайте e-LIBRARY.RU: Науч. электрон. б-ка. Режим доступа: для зарегистрир. пользователей.

References

1. Arutyunov VV. Modern problems and tasks of information security. *Vestnik Moskovskogo finansovo-yuridicheskogo universiteta MFYuA*. 2014;(3):140-146. Available from: https://elibrary.ru/wawktv [Accessed 15 June 2025]. (In Russ.).

2. Yakushkin VP, Bogdanov DA. The methodology of studying the basics of information security in military educational institutions of higher education of the troops of the National Guard of the Russian Federation. In: *Informatsionnye tekhnologii i informatsionnaya bezopasnost' v professional'noy deyatel'nosti = Information technologies and information security in professional activity: a collection of scientific articles of the IV Interuniversity Scientific and Practical Conference with international participation (Novosibirsk, February 5, 2025)*. Novosibirsk: Novosibirskiy voennyy institut imeni generala armii I. K. Yakovleva voysk natsional'noy gvardii Rossiyskoy Federatsii; 2025. p. 136-141.

3. Lukonin AV, Neshko AN. The role of information technology in the military professional training of officers of the National Guard of the Russian Federation. In: Boyko SV. (ed.) *Voyska natsional'noy gvardii Rossiyskoy Federatsii = The troops of the National Guard of the Russian Federation: past and present: proceedings of the interuniversity scientific and practical conference (on the 210th anniversary of*

the formation of the law enforcement forces and the 5th anniversary of the creation of the Rosgvardiya) (Saratov, April 7, 2021). Saratov: Saratovskiy voennyy ordena Zhukova Krasnoznamennyy institut voysk natsional'noy gvardii; 2021. p. 315-325. Available from: https://www.elibrary.ru/item.asp?id=45750522 [Accessed 12 June 2025]. (In Russ.).

4. Zhurkin VV. Features of the formation of value orientations of cadets of military universities of the National Guard of the Russian Federation. In: Pihtelev AM. (ed.) *Sotsiologicheskie znaniya v kontekste aktual'nykh problem razvitiya sotsial'nykh obshchnostey i institutov = Sociological knowledge in the context of current problems of the development of social communities and institutions: collection of scientific articles of the II All-Russian Scientific and Practical Conference (Saratov, November 29, 2024)*. Saratov: Saratovskiy voennyy ordena Zhukova Krasnoznamennyy institut voysk natsional'noy gvardii; 2024. p. 23-30. Available from: https://www.elibrary.ru/item.asp?id=80310703 [Accessed 10 June 2025]. (In Russ.).

5. Neshko AN, Lukonin AV, Gudov DV. The role and place of the discipline "Computer Science and Information Technology in professional activity" in the higher education system of the troops of the National Guard of the Russian Federation. *Izvestiya Saratovskogo voennogo instituta voysk natsional'noy gvardii = Izvestija of the Saratov Military Institute of the National Guard Troops*. 2020;(1):31-35. Available from: https://svkinio.ru/2020/1(1)/Neshko_Lukonin_Gudov.pdf [Accessed 10 June 2025]. (In Russ.).

6. Bogdanov DA. The main characteristics of the professional training of future officers of information technology units for the use of information security tools. *Akademicheskiy vestnik voysk natsional'noy gvardii Rossiyskoy Federatsii = Akademichesky Vestnik [Academic Herald] of the National Guard Troops of the Russian Federation*. 2022;(2):47-52. Available from: https://www.elibrary.ru/item.asp?id=49348729 [Accessed 15 June 2025]. (In Russ.).

7. Loginov EL. The problem of countering information attacks on Russia's critical infrastructure systems. *Vestnik Moskovskogo universiteta MVD Rossii*. 2013;(4):201-205. Available from: https://www.elibrary.ru/item.asp?edn=qiskkr [Accessed 15 June 2025]. (In Russ.).

8. Serdyuk VA. *Organizatsiya i tekhnologii zashchity informatsii: obnaruzhenie i predotvrashchenie informatsionnykh atak v avtomatizirovannykh sistemakh predpriyatiy = Organization and information security technologies: detection and prevention of information attacks in automated systems of enterprises*. Moscow: Izdatel'skiy dom Vysshey shkoly ekonomiki; 2015. Available from: https://www.elibrary.ru/item.asp?edn=qxtzdq [Accessed 13 June 2025]. (In Russ.).

9. Matvienok DV. Information exchange and information borrowing as a condition for the development of society. *Kul'turnaya zhizn' Yuga Rossii*. 2008;(2):42-44. Available from: https://www.elibrary.ru/item.asp?id=12880029 [Accessed 10 June 2025]. (In Russ.).

10. Zhuk EI. Conceptual foundations of information security. *Nauka i obrazovanie: nauchnoe izdanie MGTU imeni N. E. Baumana*. 2010;(4):7-44. Available from: https://www.elibrary.ru/item.asp?id=14571457 [Accessed 11 June 2025]. (In Russ.).

11. Kapustin FA. Information security and information protection in modern society. *Aktual'nye problemy aviatsii i kosmonavtiki*. 2016;2(12):56-58. Available from: https://www.elibrary.ru/item.asp?id=28146273 [Accessed 11 June 2025]. (In Russ.).

Информация об авторе(ах)

Д. В. Гудов – кандидат педагогических наук, доцент.

Information about the author(s)

D. V. Gudov – Candidate of Science (Pedagogy), Docent.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Статья поступила в редакцию 02.07.2025; одобрена после рецензирования 18.07.2025; принята к публикации 27.08.2025.

The article was submitted 02.07.2025; approved after reviewing 18.07.2025; accepted for publication 27.08.2025.