УДК 621.39:004.6

С. О. Константінов

А. В. Щолок

О. Р. Іщук

МЕРЕЖА, ПРОДУКТИВНІСТЬ, БЕЗПЕКА ТА ДОСТУП У ЦЕНТРАХ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ БОЙОВИХ ДІЙ ІЗ СИСТЕМОЮ JCATS

У статті досліджуються технічні аспекти побудови та експлуатації системи імітаційного моделювання бойових дій на базі JCATS (Joint Conflict and Tactical Simulation) у середовищі RHEL (Red Hat Enterprise Linux). Проаналізовано вимоги до мережевої інфраструктури, серверних ресурсів і заходів інформаційної безпеки, що впливають на достовірність і продуктивність симуляційних сценаріїв.

Окрему увагу приділено критичним мережевим параметрам – затримці, пропускній здатності, характеру трафіка – та їхньому впливу на результати моделювання. Розглянуто принципи сегментації мережі, оптимізації системних параметрів, контролю доступу й шифрування даних для забезпечення конфіденційності та цілісності інформації.

Наведено можливості масштабування та організації віддаленої взаємодії між навчальними майданчиками. Практичні рекомендації включають: мережеву сегментацію, впровадження механізмів контролю та моніторингу продуктивності серверів і клієнтів, а також використання інструментів аналізу трафіка.

К л ю ч о в і с л о в а: система моделювання, мережеве адміністрування, державна безпека, бойові дії, мережеві параметри, кібербезпека, системні параметри, командно-штабні навчання.

Постановка проблеми. У сучасних центрах імітаційного моделювання бойових дій, що функціонують на базі системи JCATS, критично важливими є стабільність мережевої інфраструктури, висока продуктивність програмно-апаратних засобів, гарантована інформаційна безпека та керований доступ користувачів. Зростання складності модельованих сценаріїв, кількості одночасних учасників, потреба у швидкому обміні даними та інтеграції з іншими системами призводять до зростання навантаження на мережеві ресурси. Це створює ризики затримок, втрат пакетів і зниження точності моделювання, що безпосередньо впливає на навчальні результати [6]. Одночасно підвищуються вимоги до інформаційної безпеки, адже центри працюють із чутливою або службовою інформацією, яка потребує захищеного передавання та контролю доступу. Отже, виникає проблема забезпечення оптимального поєднання високої пропускної здатності мережі, стабільної обчислювальної продуктивності, захищеності даних і керованого доступу у комплексах JCATS.

Аналіз останніх досліджень та публікацій. Останні дослідження та публікації свідчать про зростання уваги науковців до використання систем імітаційного моделювання у підготовці військових підрозділів, зокрема до можливостей та обмежень програмного комплексу JCATS. У працях з узагальнення досвіду застосування симуляційних засобів у Збройних Силах України [2], а також у тих, що орієнтовані на підготовку офіцерів Національної гвардії України із залученням інструментів імітаційного моделювання бойових дій [3], детально висвітлено навчальні, методичні та організаційні аспекти роботи із системами такого типу. Окремо досліджуються і технічні параметри функціонування JCATS, зокрема вплив мережевих затримок, широкомовного трафіка та навантаження на клієнтські станції під час великомасштабних сценаріїв [7]. Проте більшість цих публікацій приділяє увагу лише окремим фрагментам проблематики, тоді як комплексні питання інфраструктурної сумісності, стабільності серверних компонентів, оптимізації трафіка, сегментації мережі та забезпечення інформаційної безпеки у разі тривалої роботи системи JCATS досліджені недостатньо. Саме ці малорозкриті аспекти формують наукову новизну та визначають актуальність статті, спрямованої на пошук рішень щодо підвищення продуктивності, надійності та безпеки функціонування JCATS у сучасних центрах імітаційного моделювання.

Мета статті. Аналіз і визначення технічних рішень для забезпечення стабільної роботи, високої продуктивності та інформаційної безпеки системи JCATS під час функціонування у середовищі RHEL/Linux.

Досягнення цієї мети передбачає розроблення рекомендацій щодо побудови мережевої інфраструктури та організації безпечного доступу у центрах імітаційного моделювання бойових дій.

Виклад основного матеріалу. Сучасні центри імітаційного моделювання бойових дій є важливим елементом підготовки військових підрозділів та оперативного персоналу [1]. Основна мета таких центрів – забезпечення реалістичного відтворення динаміки бойових дій у віртуальному середовищі, що дозволяє відпрацьовувати тактичні рішення, координувати дії підрозділів та аналізувати результати [2–5].

Система JCATS (Joint Conflict and Tactical Simulation) – це інтерактивна система моделювання бойових дій (див. рис. 1), що використовується як базовий програмний комплекс для моделювання і призначена для оперативного навчання, тренувань та аналізу сценаріїв. Висока точність моделі досягається завдяки інтенсивному обміну даними між учасниками, що вимагає ретельно спроєктованої мережевої інфраструктури. Надійність, пропускна здатність і стабільність синхронізації є критичними параметрами, які безпосередньо впливають на якість симуляції. Її ефективність залежить від стабільності мережевої інфраструктури, достатньої продуктивності серверних ресурсів та належного рівня інформаційної безпеки.

У статті розглянуто ключові технічні аспекти побудови та експлуатації JCATS у середовищі RHEL (Red Hat Enterprise Linux): мережеву архітектуру, оптимізацію продуктивності, організацію безпечного доступу та принципи захисту даних.

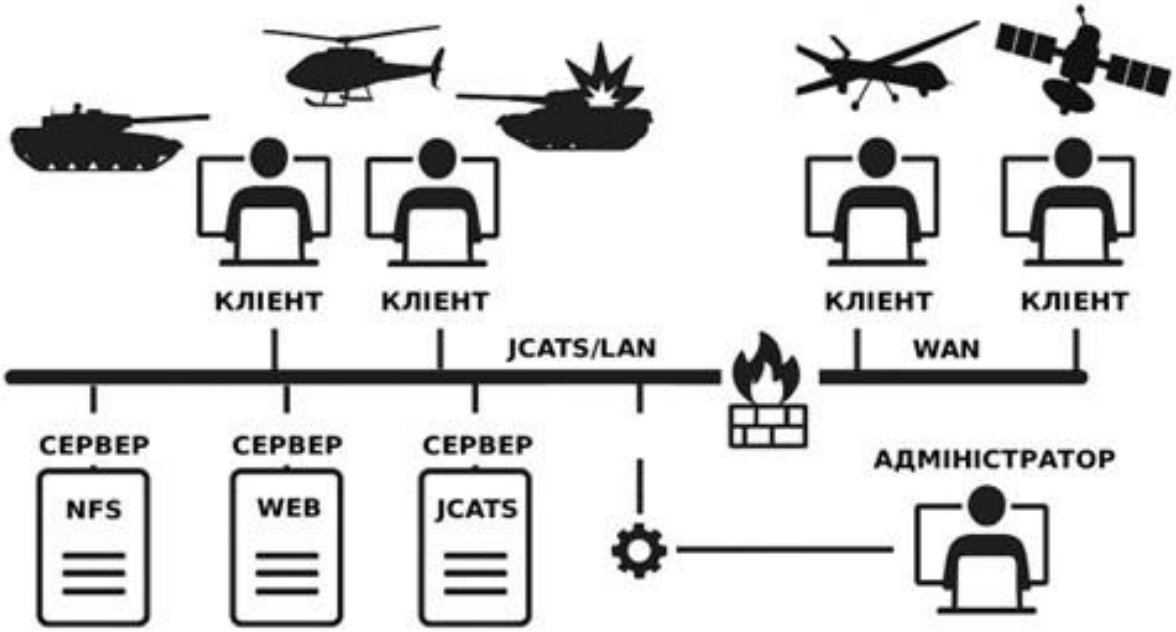

Рисунок 1 – Загальна структура мережі для систем JCATS

JCATS реалізує клієнт-серверну модель, де основні обчислення виконуються на сервері сценарію, а клієнти забезпечують інтерфейс взаємодії користувачів.

JCATS структура:

– сервер сценарію (Scenario Server) виконує симуляційні розрахунки, обробляє події та розподіляє зміни станів об’єктів;

– клієнти (Workstations) забезпечують візуалізацію, управління підрозділами та взаємодію користувачів;

– сервери даних (Data Storage / Replay) зберігають журнали подій, історію сценаріїв, медіафайли, резервні копії;

– адміністративна підсистема відповідає за моніторинг, оновлення, управління користувачами та журналювання.

Комунікація відбувається через TCP/UDP протоколи; у локальних сценаріях часто використовується broadcast для широкомовного оновлення станів. Саме тому топологія мережі повинна мінімізувати колізії і гарантувати передбачувану затримку доставки пакетів.

Для розширення кількості одночасних користувачів система JCATS може бути розподілена на декілька вузлів. У середовищі RHEL це досягається завдяки кластеризації процесів і балансуванню навантаження. Такий підхід забезпечує рівномірний розподіл ресурсів і підвищує відмовостійкість.

У випадку розміщення навчальних майданчиків у різних географічних регіонах слід забезпечити захищений канал зв'язку з контролем пропускної здатності (QoS), що дозволяє проводити спільні тренування без втрати якості синхронізації.

Рекомендовано виділяти окремі сегменти мережі для адміністративного управління, користувацьких клієнтів, серверів зберігання даних і навчальних аудиторій. Для підвищення стабільності та безпеки рекомендується розділяти трафік за функціональними зонами (табл. 1).

Таблиця 1 – Функціональні зони

Сегмент	Призначення	Підмережа
Адміністративний	Управління серверами, оновлення, моніторинг	10.10.10.0/24
Користувацький (клієнти)	Робочі станції операторів JCATS	10.10.20.0/24
Серверний (core)	Сервер сценарію, бази даних, репозиторії	10.10.30.0/24
Навчальні аудиторії / тренінгові кімнати	Тимчасові клієнти або демонстраційні станції	10.10.40.0/24

Такий підхід дає змогу:

– ізолювати контрольний трафік від навчального;

– обмежити доступ користувачів до критичних вузлів;

– спростити моніторинг і аудит мережі.

Для мінімізації конфліктів трафіка доцільно використовувати фізичну або логічну ізоляцію (рис. 2), що дозволяє знизити затримки і підвищити стабільність синхронізації між вузлами. Наприклад, логічну ізоляцію через VLAN:

– VLAN 10 – адміністративна;

– VLAN 20 – клієнтська;

– VLAN 30 – серверна;

– VLAN 40 – лабораторна.

У великих установках можна використовувати VxLAN для багатодоменних середовищ. У критичних лабораторіях рекомендується фізичне розділення комутаторів клієнтів і серверів, щоб виключити перетинання broadcast-доменів.

Зауважимо, що JCATS генерує broadcast і multicast-трафік, отже, необхідно ввімкнути IGMP Snooping та контролювати розмір доменів для уникнення «broadcast storm» [7].

JCATS генерує інтенсивний обмін даними про об'єкти, події та їхній стан, тому рекомендується мінімальна пропускна спроможність мережі на рівні 1 Гбіт/с із затримкою <5 мс між сервером і клієнтами. Затримки понад 20 мс можуть призводити до десинхронізації сценаріїв – користувачі бачитимуть різний стан поля бою. Для вимірювання продуктивності доцільно регулярно проводити тестування за допомогою iperf3, ping, tcpdump.

Продуктивність JCATS визначається не лише обчислювальною потужністю серверного обладнання, але й балансом між процесорним навантаженням, обсягом оперативної пам'яті, швидкодією дискової підсистеми та пропускною здатністю мережі.

Для оброблення великих сценаріїв рекомендується багатоядерна архітектура з можливістю розподілу процесів між вузлами. Системи з обмеженою кількістю ядер або без оптимального планування потоків можуть відчувати затримки під час обробки подій у реальному часі, що негативно впливає на точність і синхронізацію симуляцій.

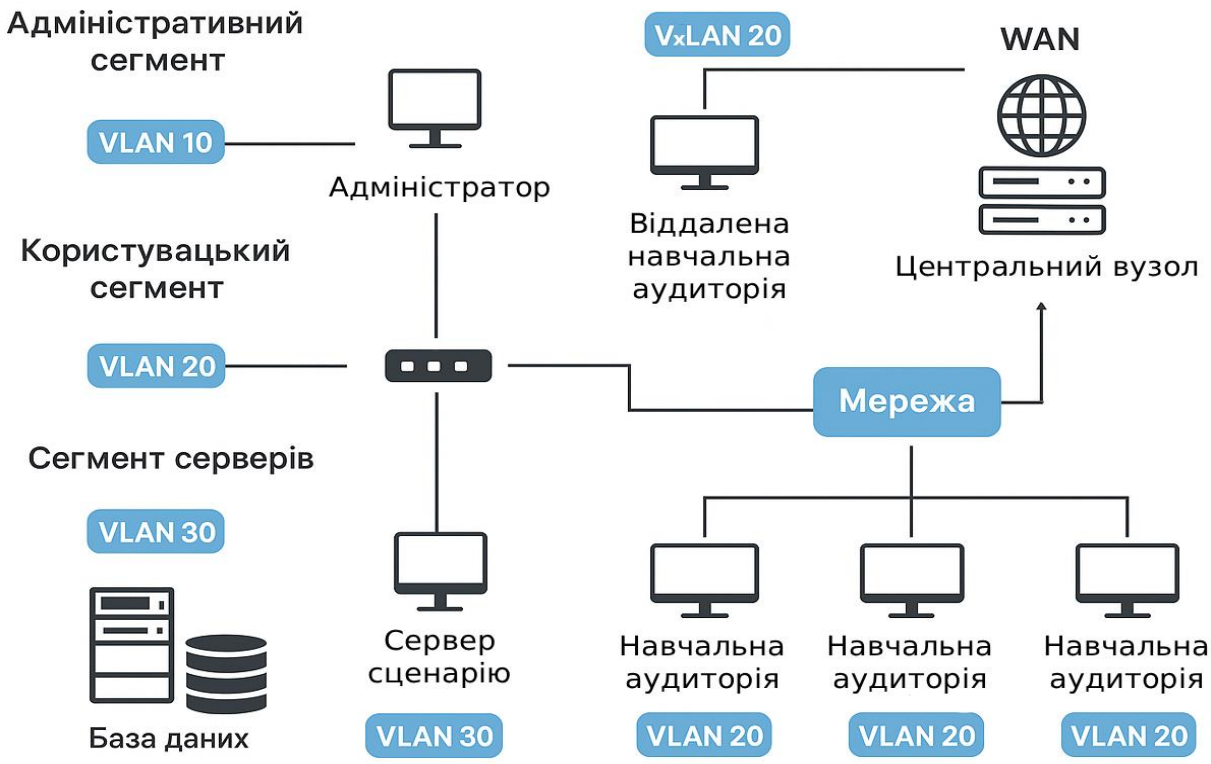

Рисунок 2 – Функціонально розділена структура мережі для систем JCATS

Тип і конфігурація накопичувачів суттєво впливають на швидкодію:

– SSD/NVMe забезпечують високі показники IOPS (input / output operations per second) та низьку латентність, тоді як HDD підходять переважно для архівування або зберігання логів;

– для JCATS рекомендовано RAID-масиви з рівнями 10 або 5, які поєднують швидкодію та відмовостійкість;

– використання параметрів монтування noatime та nodiratime зменшує кількість зайвих записів;

– для SSD доцільно використовувати команди fstrim або discard замість традиційної дефрагментації, що неефективна для твердотільних накопичувачів.

У середовищі RHEL продуктивність JCATS значною мірою залежить від правильного налаштування планувальника процесів, системних обмежень і файлової системи.

Для серверів JCATS найкраще підходять XFS або Ext4 із журналюванням. Порівняльні дослідження показують, що XFS краще масштабується при великій кількості потоків введення / виведення. Регулярна перевірка стану дискової підсистеми (iostat, smartctl) дозволяє запобігати деградації швидкодії.

Ключові метрики для відстеження (табл. 2).

Таблиця 2 – Ключові системні метрики

Метрика	Поріг	Дія
CPU Utilization per Core	>80 % протягом >5 хв	Перевірити процеси, провести профілювання
Memory Used (без кеша)	> 85 %	Аналіз споживання, перевірка витоків
I/O await	> 20 мс	Аналіз scheduler, стан диска
Network Packet Loss	> 0,5 %	Діагностика мережі, QoS
JCATS Latency p95	> 150 мс	Оптимізація сценарію або архітектури

Моніторинг системи JCATS (рис. 3) має бути безперервним і багаторівневим, охоплювати як системні ресурси, так і мережеві та прикладні метрики.

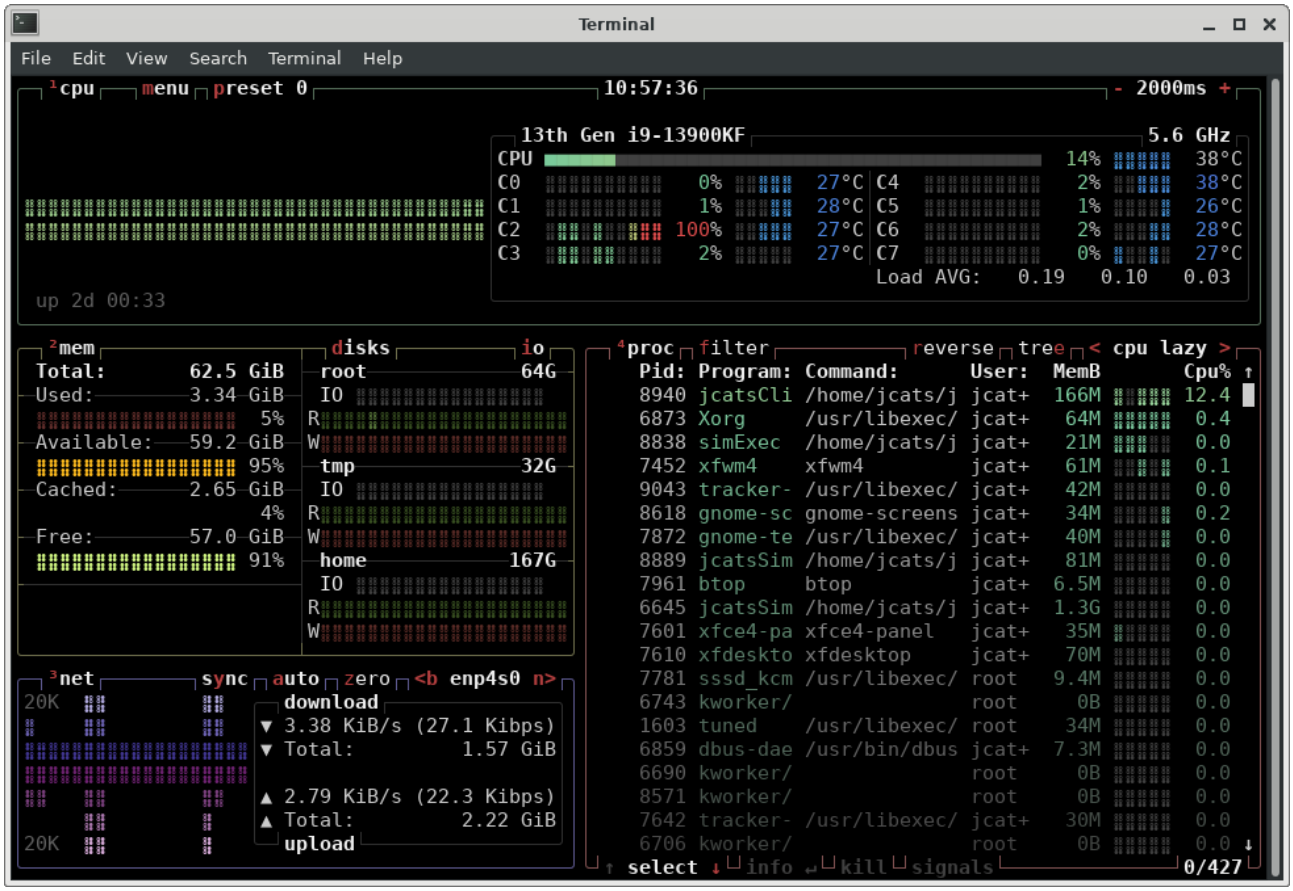

Рисунок 3 – Моніторинг системи JCATS

Процесор: завантаження по ядрах, контекстні перемикання, пріоритети задач.

Пам’ять: використання фізичної пам’яті, кешів і swap.

Дискова система: IOPS, середній час очікування (await), коефіцієнт завантаження черг.

Мережа: затримка RTT (Round Trip Time), втрати пакетів, retransmits.

Прикладний рівень: середній і 95-й процент часу реакції JCATS, кількість оброблених подій за секунду.

Для збирання та візуалізації метрик доцільно використовувати такі інструменти та архітектуру моніторингу:

– Prometheus+Grafana – для збирання та відображення системних і прикладних показників;

– Perf, iostat, vmstat, netstat, tcpdump – для точкових вимірювань і профілювання;

– Flame Graphs – для аналізу CPU hot spots у складних сценаріях.

Регулярний аналіз цих даних дозволяє своєчасно коригувати конфігурацію або планувати модернізацію обладнання.

Система JCATS оперує моделями підрозділів, сценаріями дій, даними про озброєння та результатами навчань, що належать до категорії обмеженої або конфіденційної інформації. З цієї причини політика безпеки має ґрунтуватися на багаторівневому підході (рис. 4), який охоплює як організаційні, так і технічні аспекти.

Основні елементи політики безпеки:

– обмеження доступу до адміністративних інтерфейсів через контрольні списки доступу (ACL) та багатофакторну аутентифікацію;

– контроль оновлень та перевірка джерел пакетів, що особливо важливо в середовищах RHEL; рекомендується використання репозиторіїв, підписаних цифровими сертифікатами Red Hat;

– аудит змін конфігурацій, реалізований засобами auditd та централізованими сервісами логування (наприклад, rsyslog);

– захист системного журналу від змін шляхом обмеження прав доступу, зберігання копій у захищеному сегменті або на віддаленому сервері.

Отже, організаційний рівень безпеки JCATS забезпечує контроль, відстежуваність та прозорість усіх адміністративних дій.

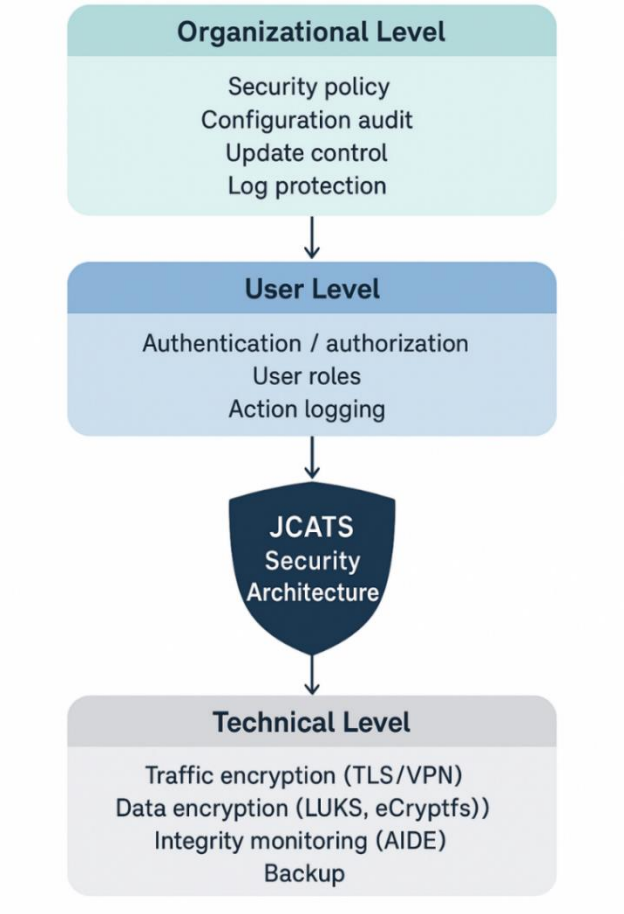

Рисунок 4 – Багаторівнева архітектура безпеки JCATS

Доступ користувачів до системи слід реалізовувати на основі обов'язкової автентифікації, централізованої автентифікації через доменну службу, що дозволяє управляти обліковими записами у єдиному домені або через локальні облікові записи з розмежуванням ролей.

Адміністратор має право лише на зміну конфігурацій та моніторинг, тоді як інженер – на створення та редагування сценаріїв, а інструктор – на їх запуск і проведення.

Усі дії користувачів фіксуються у журналах подій, що дозволяє проводити ретроспективний аналіз у разі інцидентів. Для підвищення надійності рекомендується застосовувати механізми SSSD (System Security Services Daemon) у RHEL. Отже, користувацький рівень безпеки JCATS має гарантувати цілеспрямоване управління правами доступу та мінімізувати людський фактор.

Захист інформації в JCATS здійснюється як під час передавання, так і зберігання:

– у транзиті застосовується шифрування каналів зв'язку між вузлами за допомогою протоколів TLS або SSH; у разі віддаленого доступу – VPN-з'єднання з автентифікацією сертифікатами;

– на диску використовується шифрування томів (LUKS, eCryptfs) для каталогів із навчальними сценаріями, результатами моделювання та журналами;

– інтегрований контроль цілісності за допомогою AIDE (Advanced Intrusion Detection Environment) дозволяє виявляти несанкціоновані зміни у файлах.

Резервне копіювання має виконуватися у зашифрованому вигляді, із зберіганням копій у фізично ізольованому середовищі. Технічний рівень безпеки JCATS забезпечує конфіденційність, цілісність і доступність даних відповідно до принципів CIA-тріади (Confidentiality, Integrity, Availability).

Поєднання організаційних, користувацьких та технічних заходів формує цілісну багаторівневу архітектуру безпеки JCATS, сумісну з вимогами стандартів ISO/IEC 27001 та NIST SP 800-53. Така модель дає змогу забезпечити надійний захист симуляційних даних навіть у розподіленому або хмарному середовищі [8–10].

Висновки

Мережева інфраструктура JCATS – це не просто фізична зв'язка вузлів, а керований симуляційний простір, де затримки, синхронізація та безпека безпосередньо впливають на результат навчання. Ефективна робота JCATS у центрі імітаційного моделювання бойових дій залежить від збалансованої інфраструктури, що поєднує стабільну мережу, оптимізовану продуктивність серверів, надійний захист і продуману систему доступу.

Системний підхід до адміністрування, резервування й контролю дозволяє підтримувати високу готовність комплексу до навчальних і дослідницьких завдань, мінімізуючи ризики збоїв і несанкціонованого втручання. Використання VLAN, QoS, ізоляції трафіка, резервування каналів і моніторингу дозволяє забезпечити стабільну роботу навіть у великих розподілених середовищах.

Розвиток інфраструктури може бути спрямований на розширення масштабованості та інтеграцію JCATS у комбіновані середовища. Подальші дослідження та співпраця між мережевими інженерами і фахівцями із симуляцій будуть спрямовані на розроблення методики підвищення продуктивності та захищеності, забезпечуючи надійність та ефективність симуляцій в умовах постійного технологічного розвитку.

Перелік джерел посилання

1. Analysis of the use of simulators in the ground forces of the Armed Forces of Ukraine and leading countries of the world. Research article. ResearchGate, 2025.

2. Проблеми застосування систем імітаційного моделювання у Збройних Силах України : матеріали наук.-практ. семінару (м. Київ, 28 трав. 2024 р.). Київ, 2024. С. 62.

3. Іохов О., Лаврінчук О., Горєлишев С. Використання засобів імітаційного моделювання бойових дій у процесі підготовки офіцерів Національної гвардії України. Честь і закон. 2023. № 3 (86). С. 22–31.

4. Bordunova K. I., Shcholok A. V., Ishuk O. R. Features of training jcats simulation system operators in the national guard of Ukraine. Актуальні проблеми діяльності складових сектору безпеки і оборони України в умовах особливих правових режимів: поточний стан та шляхи вирішення : зб. тез доп. II Міжнар. наук.-практ. конф., м. Харків, 20 берез. 2025 р. Харків, 2025. С. 30–31.

5. Maistrenko O. V., Bubenshchykov R. V., Stetsiv S. V. The use of simulation modelling tools in a practical training for the prospective officers of the Armed Forces of Ukraine. Information Technologies and Learning Tools. 2020. Vol. 75. No 1. Pp. 186–201.

6. Bratko A., Shevchuk V. Analysis of the use of simulation systems in the process of making management decisions. Social Development and Security. 2025. 15 (1). Pp. 88–94.

7. Нестеренко Р. В., Константінов С. О., Іщук О. Р. Вплив мережевих параметрів на великомасштабні симуляції JCATS: широкомовний трафік, контроль шторму та навантаження на процесор клієнта. Збірник наукових праць Національної академії Національної гвардії України. Харків, 2025, Вип. 1 (45). С. 94–99.

8. ISO/IEC 27031:2011. Information technology – Security techniques – Guidelines for ICT readiness for business continuity.

9. ISO/IEC 22301:2019. Security and resilience – Business continuity management systems – Requirements.

10. Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1). NIST, 2020.

Стаття надійшла до редакції 10.11.2025 р.

UDC 621.39:004.6

S. Konstantinov, A. Shcholok, O. Ishchuk

NETWORKING, PRODUCTIVITY, SECURITY AND ACCESS IN WARFARE SIMULATION CENTERS WITH JCATS SYSTEM

The article provides a comprehensive examination of the technical aspects of building, configuring, and operating the JCATS (Joint Conflict and Tactical Simulation) combat simulation system deployed in the RHEL (Red Hat Enterprise Linux) environment. It outlines the key requirements for network infrastructure, hardware resources, and cybersecurity measures that determine the quality, reliability, and stability of simulation scenarios in training centers. Significant attention is devoted to analyzing critical network parameters—packet latency, bandwidth, traffic characteristics, and intensity—which directly affect object synchronization, event accuracy, and the responsiveness of command processing within the system.

The article provides a detailed description of approaches to network segmentation, optimization of operating system parameters, and the implementation of access control policies that ensure isolation of service, user, and broadcast traffic. Emphasis is placed on the importance of applying data encryption methods and mechanisms for maintaining information integrity to ensure an appropriate level of confidentiality for simulation data. The study also reviews the scalability of JCATS in multi-node configurations and mechanisms for organizing remote interaction between training sites, particularly through secure communication channels with QoS support and load control.

Practical recommendations are provided regarding the use of performance monitoring tools for servers and client workstations, methods for analyzing network traffic, and optimization strategies for configurations used in complex, high-load scenarios. It is emphasized that the integration of these measures is aimed at improving the system's resilience, security, and overall efficiency during large-scale simulations involving numerous participants.

In conclusion, the paper notes that the rapid evolution of technology, combined with increasing demands for adaptability and security in training complexes, requires further research. This is essential for maintaining the high accuracy and overall effectiveness of JCATS under changing operational conditions and amid the growing complexity of simulated combat scenarios.

K e y w o r d s: modeling system, network administration, national security, combat operations, network parameters, cybersecurity, system parameters, command and staff exercises

Константінов Сергій Олександрович – начальник відділення програмно-технічного забезпечення та обслуговування комп'ютерної техніки центру імітаційного моделювання Національної академії Національної гвардії України.

https://orcid.org/0009-0000-7323-0390

Щолок Андрій Володимирович – начальник науково-дослідного відділення розвитку геоінформаційних систем супроводження моделей операцій, бойових та спеціальних дій центру імітаційного моделювання Національної академії Національної гвардії України.

https://orcid.org/0009-0007-6008-8832

Іщук Олександр Романович – науковий співробітник науково-дослідного відділення розвитку геоінформаційних систем супроводження моделей операцій, бойових та спеціальних дій центру імітаційного моделювання Національної академії Національної гвардії України.

https://orcid.org/0009-0001-1833-4426