

DOI [10.28925/2663-4023.2023.20.164173](https://doi.org/10.28925/2663-4023.2023.20.164173)**Негоденко Віталій Петрович**

аспірант кафедри інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0002-7678-9138

v.nehodenko.asp@kubg.edu.ua**ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ КОНФЛІКТІВ У СИСТЕМІ НАВЧАННЯ
ЗСУ ЗА ДОПОМОГОЮ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ**

Анотація. Країна перебуває в стані війни, що вимагає швидкого навчання військових підрозділів із залученням компетентного особового складу військовослужбовців, які вже мають відповідну індивідуальну підготовку, у поєднанні із інформаційними системами тренування та відпрацювання бойових завдань як на полі бою, так і за допомогою систем імітаційного моделювання. Встановлено, що впровадження сучасних інформаційних технологій та засобів імітаційного моделювання у систему бойової та оперативної підготовки підрозділів дозволяє досягти значного зниження фінансових витрат при одночасному підвищенні якості підготовки військ. Досліджено, що високий рівень інтенсивності навчально-бойової діяльності забезпечується, за рахунок застосування сучасних систем моделювання бойових дій, які дають змогу командирам та штабам відпрацювати навчальні завдання із залученням мінімально необхідної кількості особового складу, техніки та коштів, а також відпрацьовувати всі поставлені завдання віддалено в режимі реального часу. Визначено, що існує потреба в удосконаленні системи підготовки підрозділів ЗС України шляхом нарощування можливостей систем імітаційного моделювання та об'єктивного контролю ведення бойових дій, а саме використання системи HOME STATION INSTRUMENTATION TRAINING SYSTEM (США) із забезпеченням безпечної передачі даних до командних пунктів або пунктів бойового управління усіх задіяних при цьому підрозділів. Встановлено, що важливим залишається питання розробки програмного забезпечення, що дозволить об'єднати всі системи в одну базу даних в реальному часі, із врахуванням безпеки передачі даних та безконфліктної взаємодії всіх систем.

Ключові слова: системи імітаційного моделювання; командно-штабні навчання; конфлікт; суперечність; інформаційний конфлікт; система безпеки.

ВСТУП

Динаміка розвитку сучасних збройних сил суттєво змінює характер вимог щодо професійно важливих якостей військовослужбовців, ставить нові завдання щодо їх компетентності.

Аналіз досвіду навчань та заходів підготовки особового складу збройних сил провідних країн світу показує, що широке впровадження сучасних інформаційних технологій та засобів імітаційного моделювання у систему бойової та оперативної підготовки дозволяє досягти значного зниження фінансових витрат при одночасному підвищенні якості підготовки військ. При цьому командно-штабні навчання з використанням систем імітаційного моделювання стали найефективнішою формою підготовки командувачів (командирів) та органів управління всіх рівнів.

Високий рівень інтенсивності навчально-бойової діяльності забезпечується, насамперед, за рахунок застосування сучасних систем моделювання бойових дій, які дають змогу командирам та штабам відпрацювати навчальні завдання із залученням мінімально необхідної кількості особового складу, техніки та коштів. За рахунок моделювання майбутніх дій командирам в ході навчань надається можливість виявити



системні проблеми та помилки, проаналізувати їх, вивчити та вдосконалити результати рішень шляхом багаторазових повторень та тренувань із самокритичним підходом.

Сучасні інформаційні технології дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих стаціях системи імітаційного моделювання відповідно до прийнятих рішень. Але виникають конфлікти взаємодії відповідних підсистем в цілому.

Постановка проблеми. Сутність командно-штабних навчань полягає в тому, щоб за допомогою об'єднання систем імітаційного моделювання на всіх рівнях підготовки військовослужбовців, забезпечити виконання всіх функціональних обов'язків за посадою із зосередженням зусиль на: активному добуванні, вивченні, оцінюванні відомостей про актуальну обстановку на ділянці виконання бойової задачі, прогнозування її змін і можливого розвитку бою (бойових дій); аналіз отриманих відомостей щодо можливих дій супротивника, уточненні бойових планів; приховуванні та введенні в оману противника щодо стану, положення та характеру майбутніх дій; забезпеченні прийняття командиром рішень та їх оформленні; доведенні завдань до підпорядкованих штабів і підрозділів; плануванні, організації та практичній підготовці бою (бойових, спеціальних дій); безпосередньому управлінні боєм (бойовими діями) військовими частинами (підрозділами); підтриманні надійної взаємодії та управління, швидкому його відновленні; організації та здійсненні всебічного забезпечення; збереженні боєздатності підрозділів, своєчасному поповненні їх втрат на фоні складної тактичної обстановки, яка притаманна сучасному бою (бойовим, спеціальним діям). Постає завдання створення програмного забезпечення, яке б надало можливість об'єднати всі системи імітаційного моделювання в одну базу даних в реальному часі, а також забезпечити їх безконфліктну взаємодію.

Аналіз останніх досліджень і публікацій. Моделюванню навчальної діяльності з метою формування та розвитку практичних навичок курсантів (студентів) присвячена велика кількість наукових робіт. Так, у системі інформаційної безпеки дослідження [1] присвячене питанню формування криптографічних навичок студентів, робота [2] описує діяльність студентів у віртуальній лабораторії кібербезпеки. Науковці у роботі [3] пропонують застосувати міждисциплінарний підхід до формування практичних навичок кібербезпечників.

У дослідженні [4] розглянуто програмне забезпечення для імітаційного моделювання, перевірка достовірності та перевірка правильності моделей та також моделювання вхідних даних. Потрібно відмітити, в даній роботі відсутні питання взаємодії у реальних умовах із застосуванням інформаційно-комунікаційних технологій. У статті І.С. Руснака [5] розкривається питання створення інтегрованої навчально-тренувальної системи оперативної та бойової підготовки військ, що відповідає основним вимогам функціонування Збройних Сил України. У роботі О. Майстренко [6] та Л. Заїка [7] висвітлено питання застосування засобів імітаційного моделювання у процесі підготовки майбутніх офіцерів ЗСУ до виконання службових обов'язків, але при цьому не розкрито технічну реалізацію даних систем.

Таким чином, результати огляду наукових робіт свідчать про те, що дана тема є важливою, наразі актуальною.

Метою даного дослідження є аналіз сучасних інформаційних технологій, які дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих стаціях системи імітаційного моделювання відповідно до прийнятих рішень, та визначення інформаційних конфліктів у таких системах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із інструментом покращення результативності підрозділів на полі бою, є застосування систем імітаційного моделювання на будь-якому рівні підготовки військовослужбовців.

Організація бойової підготовки у збройних силах США базується на використанні методики Crawl-Walk-Run «повзти-ходити-бігти».

Ця методика від простого до складного надає змогу військовослужбовцям покращувати індивідуальні навички і здатність виконувати колективні завдання по мірі виконання календарного плану тренувань підрозділу.

Такий метод забезпечує на кожному тренувальному етапі необхідний рівень навченості для переходу на наступний, більш складний рівень.

Але підхід до проведення всіх заходів підготовки підрозділу в умовах наближених до реальних не завжди можливий. Обмежені ресурси та час вимагають від командирів креативності, розроблення інноваційних методик проведення тренувань в умовах відмінних від реальних. Досвідчені командири планують та проводять тренування з різними за рівнем управління підрозділами, де поєднується необхідна та оптимальна підготовка у набутті навичок виконувати декілька основних завдань за призначенням.

Після розроблення плану дій важливо звертати увагу на те, як проводиться тренувальний захід. В ідеалі, зважаючи на обмежений час і ресурси, всі тренувальні заходи підрозділу краще проводити в умовах, що наближені до реальних.

Сучасна технологія моделювання дозволяє бійцям брати участь у безперервному циклі навчання, щоб підтримувати високу бойову готовність, використовуючи економічно ефективні альтернативи моделювання в поєднанні з операціями в реальному часі та навчальними місіями. У США поточний розвиток живих, віртуальних і конструктивних систем Live-Virtual-Constructive (LVC) [5] для тренувань і репетицій місій, а також швидкий розвиток мережевих технологій і стандартів/архітектур протоколів сприяли створенню синтетичного середовища, де об'єднуються розподілені операції з кількома силами та навчання коаліції стали повсякденною реальністю.

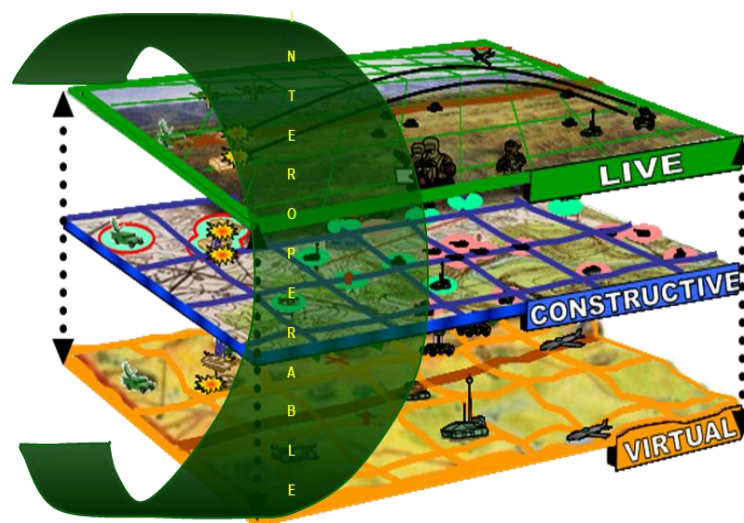


Рис. 1 Система Live-Virtual-Constructive



Дана система складається з трьох складових:

1. **Live** – реальні люди використовують реальні зразки озброєння. Військовослужбовці тренуються на тактичному полі з використанням системи лазерної імітації стрільби (типу MILES). Система імітує знищення противника та навпаки. Призначена для підготовки військовослужбовця під час тактичних занять (навчань).
2. **Virtual** – реальні люди використовують віртуальні зразки ОБТ. Військовослужбовці тренуються на комп'ютерній програмі (типу VBS-3). Система імітує виконання завдань в складі невеликого підрозділу (до роти). Призначена для підготовки молодшого командного складу та підготовки військовослужбовців для їхніх спільних дій у складі підрозділу.
3. **Constructive** – віртуальні люди використовують віртуальні зразки ОБТ. Система використовує математичні розрахунки дій військовослужбовців та ОБТ на місцевості. Дозволяє готувати штаби тактичного рівня, для яких важливо обробляти велику кількість інформації, що інтенсивно приходить з поля бою з метою вироблення рішень.

Таким чином, зв'язок між системами імітаційного моделювання та організацією індивідуальної та колективної підготовки є постійним і невід'ємним процесом тренування військ.

Використовуючи практичний підхід до підготовки підрозділів, з залученням систем імітаційного моделювання, підрозділ може одночасно проходити підготовку у реальному та синтетичному середовищі (Synthetic), де Synthetic — це комп'ютерне середовище, яке доповнює здобуття реальних навичок особового складу та командного складу шляхом імітації активних об'єктів (entities) та проєкціонування їхніх дій на реальні об'єкти (ОБТ та особовий склад).

Враховуючи досвід проведення підготовки підрозділів ЗС України у Навчальному Центрі підготовки (далі НЦПП) підрозділів на базі МЦМБ протягом 2015-2021 років, а також навчальних центрів країн-партнерів (зокрема ЗС США) вирішено удосконалити систему підготовки підрозділів ЗС України у НЦПП шляхом нарощування можливостей систем імітаційного моделювання та об'єктивного контролю ведення бойових дій, а саме використання системи HITS – HOME STATION INSTRUMENTATION TRAINING SYSTEM із забезпеченням безпечної передачі даних до віддалених командних точок [6].

HITS - це мобільна система, яка здатна покращити колективну підготовку підрозділів в режимі реального часу на стаціонарних станціях. HITS надає можливість командирам підрозділів та призначеним спостерігачам-контролерам-тренерам (ОС-Т) для надання зворотного зв'язку з навчальними підрозділами за допомогою автоматизованих систем. HITS - це інтегрована система обчислювальних пристроїв, цифрових дисплеїв карт, радіоприймачів на основі GPS, лазерних модельованих засобів залучення та реле бездротового зв'язку, які виробляють, записують та подають дані, голосові та відео файли (Рис 2).



Рис. 2 Структурна схема інтегрованого тренувального середовища

Дані щодо результатів підготовки необхідно використовувати під час проведення підсумків. Система HITS повністю інтегрована з реальною, віртуальною та конструктивною системою бойового середовища типу JCATS, VBS-3, MILES, LAZERTAG, бойової системи управління тактичної ланки «КРОПИВА», системи відображення повітряної обстановки АРМ «ВІРАЖ-ПЛАНШЕТ».

Система HITS надасть змогу проводити підготовку в Інтегрованому тренувальному середовищі LVC (**Live, Virtual, Constructive**) (Рис. 3).

Live (реальне середовище) - підрозділи займаються на штатному ОБТ:

- ТН з залученням підрозділу позначення противника, MILES, LASERTAG)
- ТН з бойовою стрільбою.

Virtual (віртуальне середовище) підрозділи (штаби) займаються у віртуальному середовищі:

- VBS-3 та аналогічні системи;
- динамічні тренажери, які діють в одній мережі (просторі).

Constructive (конструктивне середовище) командири підрозділів (штаби) керують віртуальними підрозділами відповідно ОШС:

- система імітаційного моделювання JCATS;
- бойова система управління тактичної ланки «КРОПИВА»;
- система відображення повітряної обстановки АРМ «ВІРАЖ-ПЛАНШЕТ»;
- WARSIM (США).

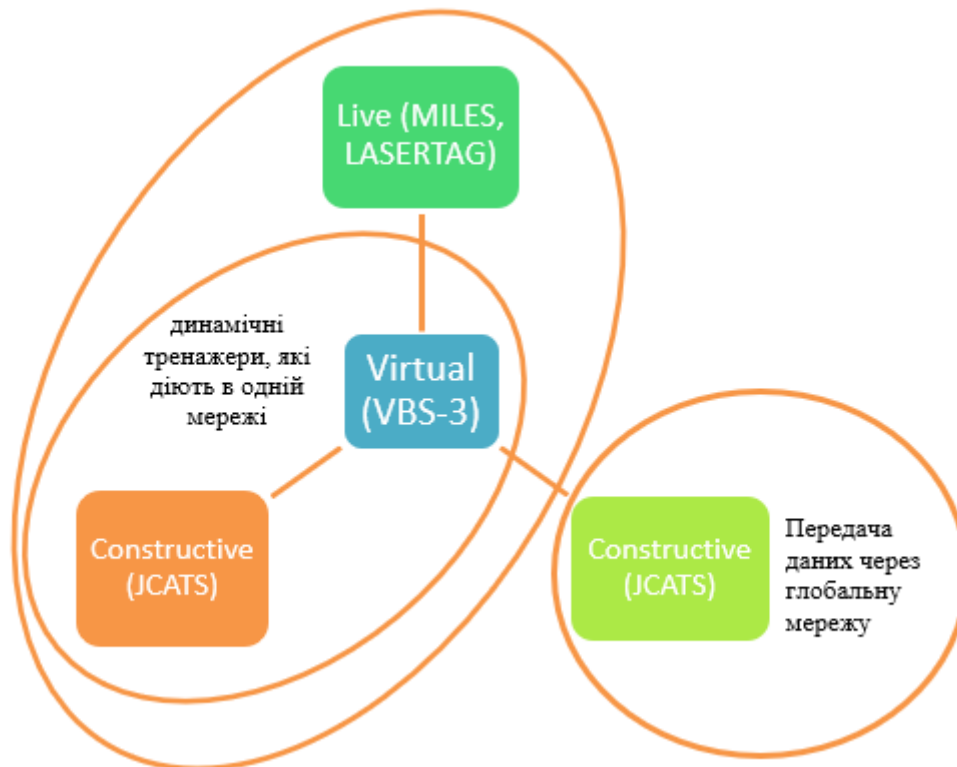


Рис. 3 Інтегроване тренувальне середовище LVC

При такому поєднанні компонентів в інтегрованому тренувальному середовищі виникає ряд проблем.

Одна з них – наявність інформаційних конфліктів між компонентами системи.

Підходи до визначення інформаційного конфлікту були дослідженні у роботі [8]. Ми згодні з вченими [9–14], які пропонують в поняття інформаційний конфлікт (кіберконфлікт) вкладати процес зіткнення сторін на етапах збору, формування, передачі, зберігання, обробки, подання та інтерпретації інформації про стан, наміри та дії.

Інформаційні конфлікти як конфлікти в інформаційних системах між впровадженими програмами або у телекомунікаційних системах між радіоелектронними засобами та системами безпеки лежать в основі системи інтегрованого тренувального середовища. Серед них виділяємо: конфлікти процесів; внутрішньомережні конфлікти; конфлікти між програмним забезпеченням та програмами, що здійснюють захист інформації; соціальні конфлікти. При побудові системи інтегрованого тренувального середовища необхідно врахувати наступні чинники:

- вивчення динаміки кожного із конфліктів;
- визначення впливу кожного конфлікту та впливу сумарної взаємодії даних конфліктів на розвиток системи;
- створення математичної моделі функціонування системи в умовах конфлікту (або конфліктів);
- управління конфліктами у даній системі.

Якщо конфлікт переростає в активну стадію, коли виникають різкі зміни та стрибкоподібні процеси, що пов'язані з інцидентами у інформаційній та кібернетичній безпеці, є логічним застосувати положення теорії катастроф [15].



Всі ці аспекти вимагають створення та удосконалення існуючого програмного забезпечення, що дозволить максимально наблизити систему до практичної візуалізації навчання курсантів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведено аналіз сучасних інформаційних технологій, які дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих стаціях системи імітаційного моделювання відповідно до прийнятих рішень. Встановлено, що найкращим рішенням є система HITS (США), яка через мережу ретрансляторів об'єднує всі моделі комп'ютерних систем в один блок, що надає можливість керівнику навчання спостерігати за навчаннями від роботи штабу бригади до дій солдата включно на тактичному полі під час проведення маневрів на одному моніторі.

Запровадження даної моделі, що поєднує реальні, віртуальні та конструктивні системи бойового середовища типу JCATS, VBS-3, MILES, LAZERTAG, бойової системи управління тактичної ланки «КРОПИВА», системи відображення повітряної обстановки АРМ «ВІРАЖ-ПЛАНШЕТ» для проведення командно-штабного навчання з залученням військ надасть можливість зменшити у декілька разів залучення озброєння та військової техніки, що в свою чергу скоротить кількість використання палива, боєприпасів та зменшить моторесурс техніки. Важливим залишається питання розробки програмного забезпечення, що дозволить об'єднати всі системи в одну базу даних в реальному часі, із врахуванням безпеки передачі даних та безконфліктної взаємодії всіх систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1 Zhdanova, Y., Spasiteleva, S., Shevchenko, S. (2019). APPLICATION OF THE SECURITY.CRYPTOGRAPHY CLASS LIBRARY FOR PRACTICAL TRAINING OF SPECIALISTS FROM THE CYBER SECURITY. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, 4(4), 44–53. <https://doi.org/10.28925/2663-4023.2019.4.4453>
- 2 Buriachok, V. L., Shevchenko, S. M., Skladannyi, P. M. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, 2(2), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
- 3 Buriachok, V., Shevchenko, S., Zhdanova Y., Skladannyi, P., (2021). INTERDISCIPLINARY APPROACH TO THE DEVELOPMENT OF IS RISK MANAGEMENT SKILLS ON THE BASIS OF DECISION-MAKING THEORY. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, 3(11), 155–165. <https://doi.org/10.28925/2663-4023.2021.11.155165>
- 4 Руснак, І.С., Шевченко, В.Л., Артемов, Ю.І. (2002). Методологічні засади створення інтегрованої навчально-тренувальної системи оперативної та бойової підготовки військ. *Наука і оборона*, 2, 29–35.
- 5 Казмірчук, Р.В. (2012). Обґрунтування пропозицій щодо впровадження в процес бойової підготовки форм і методів навчання, заснованих на використанні сучасних систем імітаційного моделювання. НДР, АСВ.
- 6 Майстренко, О. В., Бубенчиков, Р. В., Стеців, С. В. (2020). Застосування засобів імітаційного моделювання у процесі підготовки майбутніх офіцерів збройних сил України до виконання службових обов'язків. *Інформаційні технології і засоби навчання*, 75(1), 186–201.
- 7 Заїка, Л.А., Лаврінчук, О.В., Крайнов, В.О. (2021). Використання можливостей засобів імітаційного моделювання бойових дій у ході практичної підготовки органів військового управління. *Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони*, 3(42), 89–96.



- 8 Шевченко, С.М., Складанний, П.М., Негоденко, О.В., Негоденко, В.П. (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*, 2(18), 150-162. <https://doi.org/10.28925/2663-4023.2022.18.150162>
- 9 Zalcman, L, Blacklock, J., Foster, K., Lawrie, G. (2012). An Air Operations Division Live, Virtual and Constructive (LVC) Corporate Interoperability Standards Development Strategy. Fishermans Bend, Vic. : Defence Science and Technology Organisation, 74-77.
- 10 Gourley, S. R. (2012). Homestation Instrumentation Training System. ARMY.
- 11 Bocetta, S. Resolving the Conflict Between Availability and Security in IT. <https://securityboulevard.com/2022/08/resolving-the-conflict-between-availability-and-security-in-it/>
- 12 Alkubaisy, D. (2021). A Framework Managing Conflicts between Security and Privacy Requirements. https://research.brighton.ac.uk/files/25764156/Alkubaisy_Thesis.pdf
- 13 Boonstra, A., Jan de Vries. (2015). Information system conflicts: causes and types. *International Journal of Information Systems and Project Management*, 3(4), 5-20. <https://doi.org/10.12821/ijispm030401>
- 14 Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, 17(2), 245–260. <https://doi.org/10.1093/jcsl/krs018>
- 15 Shevchenko, S., Zhdanova Y., Spasiteleva, S. (2023). MATHEMATICAL METHODS IN CYBERSECURITY: CATASTROPHE THEORY. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, 3(19), 165–175. <https://doi.org/10.28925/2663-4023.2023.19.165175>

**Negodenko Vitaly Petrovych**

postgraduate student of the department of information and cybernetic security named after Professor Volodymyr Buryachko

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID: 0000-0002-7678-9138

v.nehodenko.asp@kubg.edu.ua

INVESTIGATION OF INFORMATION CONFLICTS IN THE EDUCATION SYSTEM OF THE ZSU WITH THE HELP OF SIMULATION

Abstract. The country is in a state of war, which requires rapid training of military units with the involvement of competent personnel of military personnel who already have appropriate individual training, combined with information systems of training and practicing combat tasks both on the battlefield and with the help of simulation simulation systems. It has been established that the introduction of modern information technologies and means of simulation into the system of combat and operational training of units allows to achieve a significant reduction in financial costs while at the same time increasing the quality of training of troops. It has been investigated that a high level of intensity of training and combat activities is ensured by the use of modern combat simulation systems, which enable commanders and staffs to practice training tasks with the involvement of the minimum necessary number of personnel, equipment and funds, as well as to practice all assigned tasks remotely in real time mode. It was determined that there is a need to improve the system of training units of the Armed Forces of Ukraine by increasing the capabilities of simulation modeling systems and objective control of combat operations, namely the use of the HOME STATION INSTRUMENTATION TRAINING SYSTEM (USA) system with the provision of safe data transmission to command points or combat points management of all units involved in this. It has been established that the issue of software development remains important, which will allow combining all systems into one database in real time, taking into account the security of data transmission and conflict-free interaction of all systems.

Keywords: simulation modeling systems; command and staff exercises; conflict; contradiction; information conflict; security system.

REFERENCES

- 1 Zhdanova, Y., Spasiteleva, S., Shevchenko, S. (2019). APPLICATION OF THE SECURITY.CRYPTOGRAPHY CLASS LIBRARY FOR PRACTICAL TRAINING OF SPECIALISTS FROM THE CYBER SECURITY. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 4(4), 44–53. <https://doi.org/10.28925/2663-4023.2019.4.4453>
- 2 Buriachok, V. L., Shevchenko, S. M., Skladannyi, P. M. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Security as a form of Forming Practical Skills of Students. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 2(2), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
- 3 Buriachok, V., Shevchenko, S., Zhdanova Y., Skladannyi, P., (2021). INTERDISCIPLINARY APPROACH TO THE DEVELOPMENT OF IS RISK MANAGEMENT SKILLS ON THE BASIS OF DECISION-MAKING THEORY. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 3(11), 155–165. <https://doi.org/10.28925/2663-4023.2021.11.155165>
- 4 Rusnak, I.S., Shevchenko, V.L., Artemov, Yu.I. (2002). Metodolohichni zasady stvorennia intehrovanoi navchalno-trenavalnoi systemy operatyvnoi ta boiovoi pidhotovky viisk. *Nauka i oborona*, 2, 29-35.
- 5 Kazmirchuk, R.V. (2012). Obgruntuvannia propozyzii shchodo vprovadzhennia v protses boiovoi pidhotovky form i metodiv navchannia, zasnovanykh na vykorystanni suchasnykh system imitatsiinoho modeliuвання. NDR, ASV.
- 6 Maistrenko, O. V., Bubenshchykov, R. V., Stetsiv, S. V. (2020). Zastosuvannia zasobiv imitatsiinoho modeliuвання u protsesi pidhotovky maibutnikh ofitseriv zbroinykh syl Ukrainy do vykonannia sluzhbovykh обов'язkiv. *Informatsiini tekhnologii i zasoby navchannia*, 75(1), 186-201.
- 7 Zaika, L.A., Lavrinchuk, O.V., Krainov, V.O. (2021). Vykorystannia mozhyvostei zasobiv imitatsiinoho modeliuвання boiovykh dii u khodi praktychnoi pidhotovky orhaniv viiskovoho upravlinnia. *Interaktyvni modeli rozvytku naukovo-osvitnoho prostoru u sferi bezpeky ta oborony*, 3(42), 89-96.



- 8 Shevchenko, S.M., Skladannyi, P.M., Nehodenko, O.V., Nehodenko, V.P. (2022). Doslidzhennia prykladnykh aspektiv teorii konfliktiv u systemakh bezpeky. *Kiberbezpeka: osvita, nauka, tekhnika*, 2(18), 150-162. <https://doi.org/10.28925/2663-4023.2022.18.150162>
- 9 Zalcman, L, Blacklock, J., Foster, K., Lawrie, G. (2012). *An Air Operations Division Live, Virtual and Constructive (LVC) Corporate Interoperability Standards Development Strategy*. Fishermans Bend, Vic. : Defence Science and Technology Organisation, 74-77.
- 10 Gourley, S. R. (2012). *Homestation Instrumentation Training System*. ARMY.
- 11 Bocetta, S. Resolving the Conflict Between Availability and Security in IT. <https://securityboulevard.com/2022/08/resolving-the-conflict-between-availability-and-security-in-it/>
- 12 Alkubaisy, D. (2021). *A Framework Managing Conflicts between Security and Privacy Requirements*. https://research.brighton.ac.uk/files/25764156/Alkubaisy_Thesis.pdf
- 13 Boonstra, A., Jan de Vries. (2015). Information system conflicts: causes and types. *International Journal of Information Systems and Project Management*, 3(4), 5-20. <https://doi.org/10.12821/ijispm030401>
- 14 Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, 17(2), 245–260. <https://doi.org/10.1093/jcsl/krs018>
- 15 Shevchenko, S., Zhdanova Y., Spasiteleva, S. (2023). MATHEMATICAL METHODS IN CYBERSECURITY: CATASTROPHE THEORY. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, 3(19), 165–175. <https://doi.org/10.28925/2663-4023.2023.19.165175>

