МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна наукова
праця на правах рукопису

ШАПРАН Олександр Олександрович

Прим. №_____

УДК 004.8: 687.324.072

ДИСЕРТАЦІЯ
МЕТОДИКА ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

125 – Кібербезпека
12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії.
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____Олександр ШАПРАН

Наукові керівники
САВЧЕНКО Віталій Анатолійович, доктор технічних наук, професор
ТИЩЕНКО Максим Георгійович, кандидат технічних наук, старший дослідник

Київ – 2023

АНОТАЦІЯ

Шапран О.О. Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека. – Державний університет інформаційно-комунікаційних технологій, Київ, 2023.

В сучасних умовах не викликає сумніву те, що саме технології дистанційного навчання мають розвиватися швидкими темпами. На думку експертів у 2023 – 2025 роках, очікується збільшення обсягу використання даних технологій у різних сферах суспільства приблизно в 2–4 рази в порівнянні з початком 20-х років. Це стосується і дистанційного навчання в Збройних Силах України.

Дослідження, яке виконано в межах даної дисертації, показує, що рівень ефективності, показники якості та вартості для систем дистанційного навчання продовжують покращуватися. Особлива увага приділяється заходам кібербезпеки, а саме, забезпеченню захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Даний напрям розвитку відповідає вимогам законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Це ще більше підкреслює актуальність наукових досліджень з метою підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України за рахунок ефективного реагування на потік загроз.

На теперішній час для забезпечення гарантованого рівня захищеності персональних даних користувачів системи дистанційного навчання активно

використовуються прогресивні організаційні, апаратні та програмні рішення. Аналіз закордонного та вітчизняного досвіду розробки та впровадження як систем кібербезпеки взагалі, так і систем захисту персональних даних користувачів системи дистанційного навчання свідчить про можливість підвищення їх ефективності за рахунок розвитку математичного та програмного забезпечення. Результати дослідження доводять, що найбільш актуальним в цьому напрямку є використання моделей та методів штучного інтелекту, а саме, нечіткої логіки та гібридних мереж. Незважаючи на стрімкий розвиток теорії штучного інтелекту взагалі, актуальним є завдання удосконалення існуючого та розробки нового математичного та програмного забезпечення системи захисту персональних даних користувачів системи дистанційного навчання на основі нечіткого виведення.

В сучасних науково-практичних журналах та інших наукових виданнях є інформація про використання штучного інтелекту під час здійснення кіберзлочинів. Безумовно, ця тенденція вплине на майбутнє кібератак. Дослідження показало, що у кібербезпеці використовується кілька різних методів та моделей штучного інтелекту, а саме, нечітка логіка, генетичні алгоритми, нейронні мережі та машинне навчання. Так, наприклад, найпоширеніші з методів, які використовують штучний інтелект, вирішують завдання ідентифікації та моніторингу зловмисних дій, виявлення кіберзагроз і захисту мережі організації. Варто також звернути увагу на те, що аналітик зловмисного програмного забезпечення використовує алгоритми машинного навчання для того щоб навчити систему захисту, яка побудована на теорії штучного інтелекту, виявляти шкідливі файли або підозрілі хости у мережі. Система штучного інтелекту також може відстежувати поведінку окремої людини або групи, а саме, аналізувати трафік співробітників або виявляти зміни в соціальних мережах, щоб знайти тих, хто може планувати кіберзлочини. Під час впровадження штучного інтелекту в кібербезпеку ключовими є наступні питання: як

керувати даними та як структурувати дані, щоб зробити їх доступними для програм, які забезпечують контроль людини.

Разом з класичними підходами штучного інтелекту кібербезпека також все більше використовує когнітивні технології. Когнітивні технології на основі принципів, моделей та методів штучного інтелекту є невід'ємною частиною системного підходу до кібербезпеки, в якому людський фактор керує процесом і відіграє ключову роль. Тривіальним є висновок про те, що кіберзахист постійно змінюється, так як характер загроз безпеці змінюється з кожним кроком розвитку. Аналітики вважають, що професіонали з кібербезпеки, які можуть застосувати успішні когнітивні технології, матимуть більший успіх у захисті від кібератак. Галузь також охоплює певні тенденції, які формувались роками, наприклад роль технології блокчейн, як засобу кіберзахисту та збільшення потреби в штучному інтелекті для кібербезпеки. На думку фахівців, прогнозується, що в результаті цих заходів ефективність ІТ-безпеки зросте. Варто підкреслити також те, що раніше фахівці з кібербезпеки зосереджувалися на моніторингу загроз і захисті від них. Тепер вони більше спрямовані на оцінку та зменшення ризиків, що дозволяє уникнути фрагментів програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні, які можуть завдати шкоди. Аналіз сучасного стану дозволяє зробити висновок про те, що перспективні стратегії кібербезпеки будуть зосереджені на зменшенні ризиків і оцінці ймовірності, а не на моніторингу загроз. Ці зміни створюють абсолютно нові напрями, які пов'язані з теорією штучного інтелекту.

Отже, при вирішенні проблеми кібербезпеки системи дистанційного навчання закладів ЗС України, актуальним є наукове завдання удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України на основі штучного інтелекту. Вирішенню цього завдання і присвячена дана дисертаційна робота.

Наукова новизна одержаних результатів полягає в тому, що:

вперше запропонована методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України, яка забезпечує своєчасне реагування на потік загроз та базується на основі впровадження моделей та методів нечіткої логіки та гібридних мереж. Методика поєднує моделі та методи, які спрямовані на комплексне вирішення наступних завдань: 1) ідентифікація загрози та визначення стану системи захисту персональних даних, а саме, система забезпечує захист в повному обсязі або не забезпечує захист та вимагає застосування способів та засобів, які раніше не були використані; 2) формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або, у випадку їх непридатності, формування стратегії їх удосконалення та розробки нових; 3) прогнозування стану системи захисту в майбутньому з метою попередження шкідливого впливу загроз. Практична реалізація методики дозволяє забезпечити постійний захист персональних даних користувачів системи дистанційного навчання Збройних Сил України;

удосконалено модель оцінки стану системи захисту персональних даних, яка на відміну від існуючих базується на нечіткому логічному виведенні (алгоритм Мамдані). В моделі забезпечено оптимальний метод дефазифікації, раціональна вага та кількість правил, оптимальні параметри функцій належності. Застосування методики дозволяє отримувати кількісну оцінку ефективності системи, яка необхідна для прийняття рішення щодо подальшого її удосконалення;

вперше запропоновано метод прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз, який побудований на основі технології адаптивної нейронної нечіткої мережевої системи виведення ANFIS (Adaptive Neuro-Fuzzy Inference System). Використання методу дозволяє прогнозувати ефективність системи захисту та планувати заходи щодо забезпечення підвищення захищеності персональних даних. За результатами перевірки середня похибка прогнозу 0,006 ÷ 0,26 %.

Практичне значення одержаних результатів полягає в тому, що їх реалізація доцільна в математичному та програмному забезпеченні, як складової системи управління захистом персональних даних. Впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилась на 26-28%, а час реагування на загрози захищеності даних зменшився на 28-30%.

Результати дисертаційних досліджень реалізовані в освітньому процесі Національного університету оборони України. Реалізацією отриманих результатів є розроблені методичні рекомендації щодо підвищення ефективності функціонування системи дистанційного навчання в Збройних Силах України, методичні рекомендації щодо реалізації онлайн-курсу розвитку цифрової компетентності користувачів системи дистанційного навчання Збройних Сил України та окремі навчальні питання методичної розробки “Курсу підвищення кваліфікації наукових і науково-педагогічних працівників вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти з питань організації та використання технологій дистанційного навчання в Збройних Силах України”, акти реалізації № 609/10/268 від 26.09.2023 р. та № 609/10/269 від 26.09.2023 р.

Наведені нові науково-обґрунтовані практичні рекомендації щодо підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України дозволяють розглянути можливість використання даних підходів як у інших системах дистанційного навчання, так і у різноманітних комп’ютерних системах.

Ключові слова: персональні дані, кібербезпека, захист інформації, нечітка логіка, нейронна мережа, інформація, інформаційна система, штучний інтелект, освітнє середовище, дистанційне навчання, конфіденційність, система захисту, національна безпека, телекомунікаційна система, інформаційна безпека.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Shapran O., Tyshchenko M. Features of the students' self-work organization of higher military educational institutions under the conditions of the interactive educational environment. Journal of Scientific Papers "Social development & Security", vol 6 no 4, 2018, pp. 54-62.

2. Шапран О.О., Гогонянц С.Ю., Грицай П.М. Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (34), 2019, с.29-36.

3. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Судніков Є.О., Твардовський В.Г. Методика розробки web-додатку на основі порталу Liferay. Сучасні інформаційні технології у сфері безпеки та оборони. № 2 (38), 2020, с.71-80.

4. Шапран О.О., Гогонянц С.Ю., Прокопенко А.А. Вимоги до процесу функціонування системи дистанційного навчання вищого військового закладу освіти. Scientific discussion (Praha, Czech Republic). Vol 1, No 52, 2021, 31-34 с.

5. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Махно Є.П. Модель інтелектуалізації планування часу на виконання навчального завдання у системі дистанційного навчання. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (40), 2021, с. 143-152.

6. Shapran O., Gawliczek, P., Krykun, V., Tarasenko, N., Tyshchenko, M. Computer Adaptive language testing according to NATO Stanag 6001 requirements. Advanced Education, Vol. 8(17), 2021, pp. 19-26. (**Web of Science**)

7. Шапран О., Кравченко Ю., Махно Є., Тищенко М. Модель інтелектуалізації оптимальної траєкторії проходження дистанційного

курсу. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (43), 2022, с.105 – 114.

8. Shapran O., Kyva V., Koshlan O., Krykun V., Zaika L., Sudnikov Y. The Experience of Implementing a Digital Library in the Educational and Research Activities of the National Defence University of Ukraine named after Ivan Cherniakhovskyi. TEM Journal. 2022, Vol 11, Issue 3, pp. 1128-1139. (**Scopus**)

9. Shapran O., Tyshchenko M., Sudnikov Y., Makhno Y., Gawliczek P. Distance learning system of the professional military education institution: problematic issues of formation. Journal „Civitas et Lex”, no 1(37), 2023, pp. 17-25.

10. Шапран О., Махно Є. Аналіз процесів інтелектуалізації системи дистанційного навчання у Збройних силах України. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (46), 2023, с. 107-114.

11. Шапран О. Моделі підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Телекомунікаційні та інформаційні технології. № 2 (45), 2023, с. 33-45.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Оцінювання стійкості гетерогенних мереж з використанням методів теорії перколяції: III Міжнародна науково-практична конференція «Сучасні наукові інновації» (частина II), м. Київ, 16-17 лютого 2019 р., 2 с.

13. Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Обґрунтування напрямку дослідження стійкості гетерогенних мереж до кібератак. Міжнародна науково-практична конференція «Новини науки: дослідження, наукові відкриття, високі технології» - ΛΌГOΣ, Україна, Харків, 31 березня 2019 р., 2 с.

14. Шапран О.О., Тищенко М.Г., Гогонянц С.Ю. Прогноз значень показників можливостей системи навчання на найближчу перспективу. 2-а міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних

закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2019 р., 3 с.

15. Шапран О.О., Тищенко М.Г., Гогонянц С.Ю. Особливості алгоритмізації процедур комп'ютерного адаптивного тестування. Всеукраїнська науково-методична конференції «Забезпечення якості вищої освіти», 08 – 10 квітня 2020 р., Одеська національна академія харчових технологій, 2 с.

16. Шапран О.О., Тищенко М.Г., Прокопенко А.А. Функції дистанційного навчання у системі підготовки військових фахівців. XXVIII Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. Micro CAD-2020», 14 травня 2020 р., м. Харків, Військовий інститут танкових військ НТУ "ХПІ".

17. Шапран О.О., Гогонянц С.Ю., Клочко А.О. Технології дистанційного навчання у системі військової освіти. XXIII Міжнародна науково-практична конференція "Theoretical and Practical Foundations of Social Process Management", 29-30 червня 2020 р., Сан-Франциско, США, 4 с.

18. Шапран О.О., Салкуцан С.М., Тищенко М.Г. Дистанційне навчання у Збройних Силах України. 3-а міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2020 р., с. 91-96.

19. Шапран О.О., Махно Є.П. Особливості вибору системи управління дистанційною навчальною діяльністю. 4-та міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2021 р., с.64-65.

20. Shapran O. Yudin O., Artemov V., Tyshchenko M., Makhno Y., Tarasenko N., Forecast Model of Technical State of Telecommunication System: Intelligent Statistical Data Processing. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT-2021) Conference Proceedings, pp. 165-168. (**Scopus**)

21. Шапран О.О., Тищенко М.Г., Махно Є.П. Захист даних в інтерактивному освітньому середовищі. VI науково-практична інтернет-конференція «Проблеми моделювання та розроблення інформаційних систем» 4 квітня 2022 р., м. Дрогобич, ДДПУ ім. І. Франка, – 98 с.

22. Шапран О., Судніков Є., Тарасенко Н. Захист персональних даних методом знеособлення. III науково-практичний вебінар «Забезпечення кібероборони держави» 29 вересня 2022 року м. Київ, НУОУ, 2022. – 192 с.

23. Шапран О.О., Тарасенко Н.М., Судніков Є.О., Прокопенко А.А. Впровадження цифрової бібліотеки в освітньо-наукову діяльність. Науково-технічна конференція молодих вчених “Актуальні проблеми інформаційних технологій”, КНУ ім. Т.Шевченка, 19-20 жовтня 2022 року, с. 35-36.

ABSTRACT

Shapran O.O. Methods of increasing the security of personal data of users of the distance learning system of the Armed Forces of Ukraine. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 - Cyber Security. – State University of Information and Telecommunication Technologies, Kyiv, 2023.

In today's conditions, there is no doubt that distance learning technologies must develop at a rapid pace. According to experts, in 2023-2025, the use of these technologies in various spheres of society is expected to increase approximately 2-4 times compared to the beginning of the 20s. This applies to distance learning in the Armed Forces of Ukraine.

The research conducted within this dissertation shows that the level of effectiveness, quality and cost indicators for distance learning systems continue to improve. Particular attention is paid to cyber security measures, namely, ensuring the security of personal data of users of the distance learning system of the Armed Forces of Ukraine. This direction of development meets the requirements of the European Union legislation regarding the protection of personal data of all persons within the European Union and the European Economic Area. This further emphasizes the relevance of scientific research aimed at increasing the security of personal data of users of the distance learning system of the Armed Forces of Ukraine due to effective response to the flow of threats.

Currently, advanced organizational, hardware, and software solutions are actively used to ensure a guaranteed level of security of personal data of users of distance learning systems. The analysis of foreign and domestic experience in the development and implementation of both cyber security systems in general and personal data protection systems of users of the distance learning system indicates the possibility of significantly increasing their efficiency due to the development of mathematical and software. The study showed that the most relevant in this direction is the use of models and methods of artificial intelligence, namely, fuzzy logic and hybrid networks. Despite the rapid development of the theory of artificial intelligence in general, the task of improving the existing and developing new mathematical and software systems for the protection of personal data of users of the distance learning system based on fuzzy derivation is urgent.

Modern scientific and practical journals and other scientific publications contain information about the use of artificial intelligence in cybercrimes. Undoubtedly, this trend will affect the future of cyber attacks. The study found that cybersecurity uses several different AI techniques and models, namely fuzzy logic, genetic algorithms, neural networks, and machine learning. So, for example, the most common methods that use artificial intelligence solve the tasks of identifying and monitoring malicious actions, detecting cyber threats and protecting the organization's network. It is worth noting that the malware analyst uses machine learning algorithms to teach the protection system, which is built on the theory of artificial intelligence, to detect malicious files or suspicious computers. An artificial intelligence system can also monitor the behavior of an individual or a group, namely, analyze the traffic of employees or detect changes in social networks to find those who may plan cybercrimes. When implementing artificial intelligence in cyber security, the following questions are key: how to manage data; how to structure data to make it accessible to programs that provide human control.

Along with classical AI approaches, cyber security is also increasingly using cognitive technologies. Cognitive technologies based on the principles, models and methods of artificial intelligence are an integral part of a systemic approach to cyber security, in which the human factor drives the process and plays a key role. It is trivial to conclude that cyber defense is constantly changing, as the nature of security threats changes with each step of development. Analysts believe that cybersecurity professionals who can apply successful cognitive technologies will have greater success in defending against cyberattacks. The industry has also embraced certain trends that have been building for years, such as the role of blockchain technology as a means of cyber defense and the increasing need for artificial intelligence for cybersecurity. According to experts, it is predicted that the effectiveness of IT security will increase as a result. It is worth emphasizing that previously cyber security specialists focused on

monitoring threats and protecting against them. They are now more focused on risk assessment and mitigation, avoiding pieces of software code or sequences of commands that exploit vulnerabilities in software that could cause harm. Analysis of the current state allows us to conclude that promising cyber security strategies are focused on risk reduction and probability assessment, rather than threat monitoring. These changes create completely new directions that are related to the theory of artificial intelligence.

Therefore, when solving the problem of cyber security of the distance learning system of the Armed Forces of Ukraine, the scientific task of improving existing and developing new models and methods of increasing the security of personal data of users of the distance learning system of the Armed Forces of Ukraine based on artificial intelligence is relevant. This dissertation is dedicated to solving this problem.

The scientific novelty of the obtained results is that:

for the first time, a method of increasing the security of personal data of users of the distance learning system of the Armed Forces of Ukraine was proposed, which provides an effective response to the flow of threats and is based on the implementation of models and methods of fuzzy logic and hybrid networks. The methodology combines models and methods aimed at comprehensively solving the following tasks: 1) identification of the threat and determination of the state of the personal data protection system, namely, whether the system provides full protection or does not provide protection and requires the use of methods and means that were not previously used; 2) formation of an appropriate response to the threat from the arsenal of existing methods, methods, means and procedures or, in the case of their low efficiency, formation of a strategy for improvement and development of new ones; 3) forecasting the state of the protection system in the future in order to prevent the harmful effects of threats. The practical implementation of the methodology allows for permanent protection of personal data of users of the distance learning system of the Armed Forces of Ukraine;

the model of the personal data protection system has been improved, which, unlike the existing ones, is based on fuzzy logical deduction (Mamdani algorithm). The model provides an optimal defuzzification method, rational weight and number of rules, optimal parameters of membership functions. The application of the model allows obtaining a clear quantitative assessment of the system's effectiveness, which is necessary for making a decision for further improvement;

for the first time, a method of predicting the state of the personal data protection system with the aim of preventing the harmful influence of threats was proposed, which is built on the basis of the technology of the adaptive neural fuzzy network system of ANFIS (Adaptive Neuro-Fuzzy Inference System). Using the method allows you to predict the effectiveness of the protection system and plan measures to ensure the improvement of the security of personal data. According to the test results, the average forecast error is 0,006 ÷ 0,26 %.

The practical significance of the obtained results is that their implementation is expedient in mathematical and software as a component of the personal data protection management system. The implementation of the results of the dissertation research made it possible to increase the effectiveness of personal data protection in the distance learning system of the Armed Forces of Ukraine, namely, security during crisis periods improved by 26-28%, and response time to data security threats - by 28-30%.

The results of dissertation research are implemented in the educational process of the Distance Learning Scientific Center of the National Defense University of Ukraine during the organization and conduct of the training course for scientific and pedagogical workers, acts of implementation are No. 609/10/268 dated 26.09.2023 and No. 609/10/269 dated 26.09.2023.

The new scientifically based practical recommendations for increasing the security of personal data of users of the distance learning system of the Armed

Forces of Ukraine allow us to consider the possibility of using these approaches both in other distance learning systems and in various computer systems.

Keywords: personal data, cyber security, information protection, fuzzy logic, neural network, information, information system, artificial intelligence, educational environment, distance learning, privacy, protection system, security, telecommunication system, information security.

LIST OF AUTHOR'S PUBLICATIONS

Scientific papers, in which the main scientific results of the dissertation are published:

1. Shapran O., Tyshchenko M. Features of the students' self-work organization of higher military educational institutions under the conditions of the interactive educational environment. Journal of Scientific Papers "Social development & Security", vol 6 no 4, 2018, pp. 54-62.

2. Shapran O.O., Hogonyants S.Yu., Hrytsai P.M. General provisions of the methodology for assessing the level of military danger based on taxonomic methods. Modern information technologies in the field of security and defense. No. 1 (34), 2019, pp. 29-36.

3. Shapran O.O., Kravchenko Yu.V., Tyshchenko M.G., Sudnikov E.O., Tvardovskyi V.G. Web application development methodology based on the Liferay portal. Modern information technologies in the field of security and defense. No. 2 (38), 2020, pp. 71-80.

4. Shapran O.O., Hogonyants S.Yu., Prokopenko A.A. Requirements for the process of functioning of the distance learning system of a higher military educational institution. Scientific discussion (Prague, Czech Republic). Vol 1, No 52, 2021, pp. 31-34.

5. Shapran O.O., Kravchenko Yu.V., Tyshchenko M.G., Makhno E.P. A model of intellectualization of planning time for the completion of an educational

task in the distance learning system. Modern information technologies in the field of security and defense. No. 1 (40), 2021, pp. 143-152.

6. Shapran O., Gawliczek, P., Krykun, V., Tarasenko, N., Tyshchenko, M. Computer Adaptive language testing according to NATO Stanag 6001 requirements. Advanced Education, Vol. 8(17), 2021, pp. 19-26. (Web of Science)

7. Shapran O., Kravchenko Yu., Makhno E., Tyshchenko M. The model of intellectualization of the optimal trajectory of distance course completion. Modern information technologies in the field of security and defense. No. 1 (43), 2022, pp. 105 – 114.

8. Shapran O., Kyva V., Koshlan O., Krykun V., Zaika L., Sudnikov Y. The Experience of Implementing a Digital Library in the Educational and Research Activities of the National Defense University of Ukraine named after Ivan Cherniakhovskyi. TEM Journal. 2022, Vol 11, Issue 3, pp. 1128-1139. (**Scopus**)

9. Shapran O., Tyshchenko M., Sudnikov Y., Makhno Y., Gawliczek P. Distance learning system of the professional military education institution: problematic issues of training. Journal "Civitas et Lex", no. 1(37), 2023, pp. 17-25.

10. Shapran O., Makhno E. Analysis of processes of intellectualization of the distance learning system in the Armed Forces of Ukraine. Modern information technologies in the field of security and defense. No. 1 (46), 2023, pp. 107-114.

11. Shapran O. Methodology for increasing the security of personal data of users of the distance learning system of the Armed Forces of Ukraine. Modern information technologies in the field of security and defense. No. 2 (45), 2023, pp. 33-45.

Scientific works certifying the approbation of the dissertation materials:

12. Shapran O.O., Hogonyants S.Yu., Melnyk Y.V. Evaluation of the stability of heterogeneous networks using percolation theory methods.: III International Scientific and Practical Conference "Modern Scientific Innovations" (Part II), Kyiv, February 16-17, 2019, 2 p.

13. Shapran O.O., Hogonyants S.Yu., Melnyk Y.V. Justification of the research direction of the resistance of heterogeneous networks to cyber attacks. International scientific and practical conference "News of science: research, scientific discoveries, high technologies" - ΛΌΓΟΣ, Ukraine, Kharkiv, March 31, 2019, 2 p.

14. Shapran O.O., Tyshchenko M.G., Hogonyants S.Yu. Forecast of the values of indicators of the capabilities of the training system for the near future. 2nd international scientific and practical conference "Problems of implementing distance learning in the educational process of higher military educational institutions (military units of higher education institutions)", Ivan Chernyakhovsky National Educational Institution, Kyiv, 2019, 3 p.

15. Shapran O.O., Tyshchenko M.G., Hogonyants S.Yu. Peculiarities of algorithmization of computer adaptive testing procedures. All-Ukrainian Scientific and Methodological Conference "Quality Assurance of Higher Education", April 8-10, 2020, Odesa National Academy of Food Technologies, 2 p.

16. Shapran O.O., Tyshchenko M.G., Prokopenko A.A. Distance learning functions in the training system of military specialists. XXVIII International scientific and practical conference "Information technologies: science, engineering, technology, education, health. Micro CAD-2020", May 14, 2020, Kharkiv, Military Institute of Tank Forces of NTU "KhPI".

17. Shapran O.O., Hogonyants S.Yu., Klochko A.O. Distance learning technologies in the military education system. XXIII International Scientific and Practical Conference "Theoretical and Practical Foundations of Social Process Management", June 29-30, 2020, San Francisco, USA, 4 p.

18. Shapran O.O., Salkutsan S.M., Tyshchenko M.G. Distance learning in the Armed Forces of Ukraine. 3rd international scientific and practical conference "Problems of implementing distance learning in the educational process of higher military educational institutions (military units of higher education institutions)", Ivan Chernyakhovsky National Educational Institution, Kyiv, 2020, p. 91-96.

19. Shapran O.O., Makhno E.P. Peculiarities of choosing a system for managing distance learning activities. 4th international scientific and practical conference "Problems of implementing distance learning in the educational process of higher military educational institutions (military units of higher education institutions)", Ivan Chernyakhovsky National Educational Institution, Kyiv, 2021, pp. 64-65.

20. Shapran O. Yudin O., Artemov V., Tyshchenko M., Makhno Y., Tarasenko N. Forecast Model of Technical State of Telecommunication System: Intelligent Statistical Data Processing. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT-2021) Conference Proceedings, pp. 165-168. (**Scopus**)

21. Shapran O.O., Tyshchenko M.G., Makhno E.P. Data protection in an interactive educational environment. VI scientific and practical internet conference "Problems of modeling and development of information systems" April 4, 2022, Drohobych, DDPU named after I. Franka, 98 p.

22. Shapran O., Sudnikov E., Tarasenko N. Protection of personal data by the method of depersonalization. III scientific and practical webinar "Ensuring cyber defense of the state" on September 29, 2022, Kyiv, NUOU, 2022. 192 p.

23. Shapran O.O., Tarasenko N.M., Sudnikov E.O., Prokopenko A.A. Implementation of the digital library in educational and scientific activities. Scientific and technical conference of young scientists "Actual problems of information technologies", KNU named after T. Shevchenko, October 19-20, 2022, pp. 35-36.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 21

ВСТУП 22

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ 31

1.1. Аналіз сучасних та перспективних систем дистанційного навчання .. 31

1.2. Аналіз технологій захисту персональних даних в системах дистанційного навчання 38

1.3. Постановка наукового завдання 47

Висновки до розділу 1 50

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ 52

2.1. Обґрунтування впровадження штучного інтелекту в методи, засоби та процедури кібербезпеки та захисту персональних даних 52

2.2. Обґрунтування концепції підвищення захищеності персональних даних на основі штучного інтелекту 62

2.3. Розробка методики підвищення захищеності персональних даних на основі моделей та методів нечіткої логіки та гібридних мереж 64

2.4. Розробка моделі системи захисту персональних даних 69

Висновки до розділу 2 93

РОЗДІЛ 3. РОЗРОБКА МЕТОДУ ПРОГНОЗУВАННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ

ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ НА ОСНОВІ АДАПТИВНОЇ СИСТЕМИ НЕЙРО-НЕЧІТКОГО ВИВЕДЕННЯ…….98

3.1. Обґрунтування доцільності застосування методу прогнозування на основі нейро-нечіткого логічного виведення..... 98

3.2. Розробка методу прогнозування стану системи захисту персональних даних на основі адаптивної системи нейро-нечіткого виведення 100

Висновки до розділу 3 109

РОЗДІЛ 4. РЕКОМЕНДАЦІЇ ЩОДО ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ НАУКОВИХ РЕЗУЛЬТАТІВ..... 111

4.1. Рекомендації щодо реалізації розроблених наукових результатів 111

4.2. Комп’ютерне моделювання елементів захисту системи дистанційного навчання 123

4.3. Дослідження ефективності методики підвищення захищеності персональних даних в системі дистанційного навчання Збройних Сил України..... 128

Висновки до розділу 4 134

ВИСНОВКИ..... 138

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 142

ДОДАТКИ..... 163

Додаток А..... 163

Додаток Б 167

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВВНЗ – вищий військовий навчальний заклад;

ДН – дистанційне навчання;

ДУІКТ – Державний університет інформаційно-комунікаційних технологій;

ЗСУ – Збройні Сили України;

ІС – інформаційна система;

ІТ – інформаційні технології;

НУОУ – Національний університет оборони України;

ПЗ – програмне забезпечення;

ПДК – персональні дані користувачів;

СДН – система дистанційного навчання;

ШІ – штучний інтелект;

E-learning – електронне навчання;

ІКТ – інформаційно-комунікаційна технологія;

LMS – система управління навчанням;

LCMS – система управління навчальним контентом.

ВСТУП

Актуальність теми. 28 січня 1981 року було підписано Конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Конвенція стала першим міжнародним нормативно-правовим актом у сфері захисту персональних даних, який визначив механізми захисту прав людини та недоторканність її особистого життя, а також надав визначення поняття «персональні дані». До персональних даних відносять будь-які відомості, за якими ідентифікується або може бути ідентифікована фізична особа, зокрема: прізвище, ім'я, по батькові, дата і місце народження, паспортні дані, адреса, освіта, телефон, національність, сімейний стан, релігійні та світоглядні переконання, стан здоров'я, матеріальний стан, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому професійному, діловому та інших сферах життя особи (за винятком даних щодо виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органу місцевого самоврядування) тощо. Вказаний перелік не є вичерпним. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може оброблятися в тому числі поширюватись тільки за їх згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки.

Дослідження, яке виконано в межах даної дисертації показує, що рівень ефективності, показники якості та вартості для систем дистанційного навчання ЗС України продовжують покращуватися, але робота щодо удосконалення продовжується. Особлива увага приділяється заходам кібербезпеки, а саме, забезпечення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України.

Даний напрям розвитку відповідає вимогам законодавства України та Європейського Союзу та базується на перспективних програмно-апаратних та організаційних методах, способах та процедурах. Це підкреслює актуальність наукових досліджень з метою підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України за рахунок ефективного реагування на потік загроз.

На теперішній час для забезпечення гарантованого рівня захищеності персональних даних користувачів системи дистанційного навчання активно використовують засоби безпеки мереж, включаючи брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та технології шифрування. Існує тенденція постійної зміни кіберзагроз та кібератак, а це в свою чергу вимагає збільшення уваги до нових розробок з кібербезпеки, в тому числі для захисту персональних даних користувачів системи дистанційного навчання ЗС України. Забезпечення високого рівня ефективності таких розробок потребує сучасних, креативних підходів, з яких найбільш доцільним є той, що заснований на штучному інтелекті. Варто зазначити те, що існуюча стратегія кібербезпеки спрямована в основному на моніторинг загроз і захист від них. Перспективна стратегія кібербезпеки має бути спрямована на оцінку та зменшення ризиків, що дозволяє уникнути фрагментів шкідливого програмного коду. Отже, аналіз сучасного стану дає висновок про те, що перспективні стратегії кібербезпеки зосереджені мають бути не на моніторингу загроз, а на зменшенні ризиків цих загроз. Такі зміни створюють абсолютно нові тенденції, які тісно пов’язані з використанням штучного інтелекту.

Аналіз закордонного та вітчизняного досвіду розробки та впровадження як систем кібербезпеки в загалі, так і систем захисту персональних даних користувачів системи дистанційного навчання свідчить про можливість підвищення їх ефективності за рахунок розвитку математичного та програмного забезпечення. Дослідження показало, що

найбільш актуальним в цьому напрямку є використання моделей та методів штучного інтелекту, а саме, нечіткої логіки та гібридних мереж. Незважаючи на стрімкий розвиток теорії штучного інтелекту взагалі, актуальним залишається завдання удосконалення існуючого та розробки нового математичного та програмного забезпечення підсистеми захисту персональних даних користувачів системи дистанційного навчання ЗС України на основі нечіткого виведення.

Проблеми розвитку дистанційного навчання ЗС України та кіберзахисту відповідних інформаційних технологій, зокрема системи захисту персональних даних, розглядали та досліджували в своїх працях такі вітчизняні вчені як В.Б. Толубко, В.А. Савченко, О.Г. Оксіюк та інші.

Отже, при вирішенні проблеми кібербезпеки системи дистанційного навчання закладів ЗС України, актуальним є *наукове завдання* удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України на основі штучного інтелекту. Вирішенню цього завдання і присвячена дана дисертаційна робота.

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана відповідно до європейських та вітчизняних нормативно-правових актів про захист персональних даних та організацію кібербезпеки, у відповідності до Положення про дистанційне навчання в Національному університеті оборони України імені Івана Черняховського (2017 р.). Матеріали роботи реалізовані в науково-дослідних роботах: “Обґрунтування доцільного варіанту побудови системи дистанційного навчання вищого військового навчального закладу” (шифр, “Система-ДН”, № державної реєстрації 0120U103270), 2021 р.; “Удосконалення системи дистанційного навчання Збройних Сил України: цифровізація та інтелектуалізація” (шифр, “Технології-ДН”, № державної реєстрації 0122U200401), 2023 р.; а також у відповідності до планів наукової

роботи та науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій та Національного університету оборони України.

Мета і завдання дослідження.

Мета дослідження – підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України.

Для досягнення поставленої мети визначені наступні **окремі завдання** дослідження:

проаналізувати сучасний стан захищеності персональних даних користувачів системи дистанційного навчання ЗС України;

дослідити сучасні та перспективні методи, способи та процедури захисту персональних даних користувачів систем дистанційного навчання;

розробити моделі та методи підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України;

розробити рекомендації щодо застосування запропонованих наукових результатів. Перевірити достовірність розроблених моделей та методів.

Об'єкт дослідження − процес захисту персональних даних користувачів системи дистанційного навчання Збройних Сил України.

Предмет дослідження – моделі та методи підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України на основі штучного інтелекту.

Методи досліджень. Для досягнення поставленої в роботі мети використано методи дослідження на основі системного підходу з застосуванням моделей і методів кібербезпеки, математичної логіки, теорії множин, штучного інтелекту: нечіткої логіки та нечітких нейронних мереж. Для вирішення наукового завдання використано системний підхід. Методика проведення експерименту та перевірки достовірності розроблених наукових положень реалізована на основі методів комп'ютерного моделювання.

Наукова новизна одержаних результатів полягає в тому, що:

вперше запропонована методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України, яка забезпечує своєчасне реагування на потік загроз та базується на основі впровадження моделей та методів нечіткої логіки та гібридних мереж. Методика поєднує моделі та методи, які спрямовані на комплексне вирішення наступних завдань: 1) ідентифікація загрози та визначення стану системи захисту персональних даних, а саме, система забезпечує захист в повному обсязі або не забезпечує захист та вимагає застосування способів та засобів, які раніше не були використані; 2) формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або, у випадку їх непридатності, формування стратегії їх удосконалення та розробки нових; 3) прогнозування стану системи захисту в майбутньому з метою попередження шкідливого впливу загроз. Практична реалізація методики дозволяє забезпечити постійний захист персональних даних користувачів системи дистанційного навчання Збройних Сил України;

удосконалено модель оцінки стану системи захисту персональних даних, яка на відміну від існуючих базується на нечіткому логічному виведенні (алгоритм Мамдані). В моделі забезпечено оптимальний метод дефазифікації, раціональна вага та кількість правил, оптимальні параметри функцій належності. Застосування методики дозволяє отримувати кількісну оцінку ефективності системи, яка необхідна для прийняття рішення щодо подальшого її удосконалення;

вперше запропоновано метод прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз, який побудований на основі технології адаптивної нейронної нечіткої мережевої системи виведення ANFIS (Adaptive Neuro-Fuzzy Inference System). Використання методу дозволяє прогнозувати ефективність системи захисту

та планувати заходи щодо забезпечення підвищення захищеності персональних даних. За результатами перевірки середня похибка прогнозу 0,006 ÷ 0,26 %.

Практичне значення одержаних результатів полягає в тому, що їх реалізація доцільна в математичному та програмному забезпеченні, як складової системи управління захистом персональних даних. Впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилась на 26-28%, а час реагування на загрози захищеності даних зменшився на 28-30%.

Результати дисертаційних досліджень реалізовані в освітньому процесі Національного університету оборони України. Реалізацією отриманих результатів є розроблені методичні рекомендації щодо підвищення ефективності функціонування системи дистанційного навчання в Збройних Силах України, методичні рекомендації щодо реалізації онлайн-курсу розвитку цифрової компетентності користувачів системи дистанційного навчання Збройних Сил України та окремі навчальні питання методичної розробки “Курсу підвищення кваліфікації наукових і науково-педагогічних працівників вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти з питань організації та використання технологій дистанційного навчання в Збройних Силах України”, акти реалізації № 609/10/268 від 26.09.2023 р. та № 609/10/269 від 26.09.2023 р.

Наведені нові науково-обґрунтовані практичні рекомендації щодо підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України дозволяють розглянути можливість використання даних підходів як у інших системах дистанційного навчання, так і у різноманітних комп’ютерних системах.

Особистий внесок здобувача. Основні результати дисертаційних досліджень отримані автором особисто. В роботах, опублікованих у співавторстві, автору належить: у [1] здійснено аналіз особливості організації самостійної роботи курсантів (слухачів) вищих військових навчальних закладів в умовах інтерактивного освітнього середовища; у [2] розроблено модель оцінювання рівня небезпеки на основі таксономічних методів; у [3] запропоновано концептуальну модель розробки web-додатку на основі порталу Liferay; у [4] обгрунтовано вимоги до захисту персональних даних користувачів системи дистанційного навчання вищого військового навчального закладу; у [5] розроблено методику інтелектуалізації процедури планування часу на виконання навчального завдання у системі дистанційного навчання на основі алгоритму Мамдані; у [6] обгрунтовано вимоги до системи дистанційного навчання; у [7] розроблено методику та алгоритм інтелектуалізації оптимальної траєкторії проходження дистанційного курсу; у [8] розроблено практичні рекомендації до системи дистанційного навчання; у [9] здійснено аналіз проблем кібербезпеки системи дистанційного навчання; у [10] досліджено напрями інтелектуалізації в освіті.

Апробація результатів дисертації. Результати досліджень, які отримані у ході виконання дисертаційної роботи, доповідалися на міжнародних та всеукраїнських науково-технічних конференціях, а також на засіданнях наукового центру дистанційного навчання Національного університету оборони України та кафедри систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій: III Міжнародна науково-практична конференція «Сучасні наукові інновації» (частина II), м. Київ, 16 - 17 лютого 2019 р.; Міжнародна науково-практична конференція «Новини науки: дослідження, наукові відкриття, високі технології», м. Харків, 31 березня 2019р.; 2-а міжнародна науково-практична конференція «Проблеми

впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2019 р.; Всеукраїнська науково-методична конференції «Забезпечення якості вищої освіти», Одеська національна академія харчових технологій, 08 – 10 квітня 2020 р.; XXVIII Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. Micro CAD-2020», 14 травня 2020 р., м. Харків; XXIII Міжнародна науково-практична конференція «Theoretical and Practical Foundations of Social Process Management», 29-30 червня 2020 р., м. Сан-Франциско, США; 3-а міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2020 р.; 4-та міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2021 р.; 3-я Міжнародна конференція IEEE з передових тенденцій теорії інформації (ATIT-2021), грудень 2021р., м. Київ; VI науково-практична інтернет-конференція «Проблеми моделювання та розроблення інформаційних систем» 4 квітня 2022 р., м. Дрогобич; III науково-практичний вебінар «Забезпечення кібероборони держави» 29 вересня 2022 року м. Київ; Науково-технічна конференція молодих вчених "Актуальні проблеми інформаційних технологій", КНУ ім. Т. Шевченка, 19–20 жовтня 2022 р.

Публікації. Основні результати дисертаційної роботи відображені у 23 наукових працях, серед них: 11 статей, опублікованих у періодичних виданнях, що входять до переліку видань МОН України для публікацій результатів досліджень з технічних наук (з них 2 у виданнях, які індексуються у наукометричних базах Scopus та Web of Science, а також 1 у

періодичному науковому виданні держави, яка входять до Європейського Союзу), 12 матеріалах науково-технічних конференцій (з яких 1 індексовані у наукометричній базі Scopus). Додатково матеріали та результати роботи опубліковані у двох звітах з НДР.

Структура і обсяг дисертації. Дисертація загальним обсягом 170 сторінок машинописного тексту складається з вступу, чотирьох розділів, висновків, переліку використаних джерел з 159 найменувань. Дисертація містить 44 рисунки та 12 таблиць. Ілюстрації, таблиці, перелік використаних джерел та додаток займають 30 сторінок тексту.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

1.1. Аналіз сучасних та перспективних систем дистанційного навчання

Дослідження свідчать, що в останні роки дистанційне навчання розвивається бурхливими темпами. Це в першу чергу пов’язано з розвитком інформаційно-комунікаційних технологій та обмеженістю існуючих закладів освіти забезпечити безпеку учасникам освітнього процесу в умовах пандемії та війни.

Дистанційне навчання – це особлива форма цілеспрямованого процесу засвоєння знань, умінь та навичок, відмінною особливістю якої є взаємодія територіально рознесених учасників навчання у специфічному інформаційно-освітньому середовищі, створеному на основі синтезу сучасних педагогічних та інформаційних технологій [27]. На даний час як в системі освіти України, так і в багатьох країнах світу швидким темпом впроваджуються технології дистанційного навчання. Об’єктивними факторами для цього є:

стрімкий розвиток інформаційно-комунікаційних технологій;

можливість інтерактивної взаємодії учасників освітнього процесу;

фінансова та часова економія;

необхідність бути конкурентоспроможним на ринку праці в умовах глобальної інформатизації [62].

Дистанційне навчання дає можливість вирішення низки деяких проблем, властивих традиційному способу навчання. Головною перевагою

такого навчання є доступність інформаційних ресурсів, які дозволяють учасникам освітнього процесу отримувати необхідну інформацію незалежно від часу та простору. Така форма навчання реалізується за допомогою систем дистанційного навчання. У світі розроблені й успішно використовуються системи дистанційного навчання, що пропонують послуги з вивчення різних навчальних програм і курсів [56].

Система дистанційного навчання Збройних Сил України – підсистема військової освіти, що є сукупністю адміністративного персоналу, підрозділів дистанційного навчання, слухачів, які навчаються за дистанційною формою навчання або з використанням технологій дистанційного навчання та науково-педагогічних працівників, взаємодіючих з метою організації та здійснення дистанційного освітнього процесу в єдиному інформаційно-освітньому середовищі [27].

В умовах інтенсивного впровадження ІТ-рішень в освіті, з’явилися програмні продукти різного призначення, які поділяють на такі групи: авторські програмні продукти – Authoring Packages; системи управління навчанням – Learning Management Systems (LMS); системи управління контентом – Content Management Systems (CMS); системи управління навчанням і навчальним контентом (Learning Content Management Systems – LCMS); системи підтримки навчання (Learning Support Systems – LSS); освітні платформи (Learning Platforms – LP); віртуальні середовища навчання (Virtual Learning Environments – VLE).

Найбільш популярним програмним забезпеченням в умовах реалізації дистанційного навчання у ВВНЗ є LMS. Значний досвід використання СДН, технологічна реалізація яких будується на базі LMS, дозволив виділити загальний набір послуг, що дозволяють вирішувати дидактичні завдання, що відповідає так званому принципу «технологічної повноти» інформаційно-освітнього середовища [56,65,68-75]:

сервіси групи налаштування параметрів функціонування системи дистанційного навчання (ідентифікація, розмежування прав доступу до навчальних та організаційних матеріалів залежно від статусу користувача, формування навчальних груп, формування звітів);

послуги групи подання навчальних матеріалів (створення та редагування контенту, включення навчальних матеріалів, застосування шаблонів дизайну);

послуги групи управління процесом навчання (автоматизація процесів формування розкладу контрольних заходів, оцінювання результатів тестування, накопичення історії та статистики навчання).

Незважаючи на можливість побудови повноцінної системи дистанційного навчання на базі LMS та різноманіття пропонованих інструментів, досвід використання подібних систем визначив низку властивих їм обмежень:

необхідність побудови навчального курсу у рамках логіки середовища, що обмежує можливості індивідуалізації освітнього процесу;

надмірність інструментальних засобів, що не використовуються на практиці ні слухачами, ні викладачем, що зумовлює громіздкість використання LMS;

проблеми реалізації спільної діяльності слухачів у мережі і, як наслідок, неможливість паралельної роботи над документом чи проектом групи користувачів;

відсутність підтримки концепції WEB останніх оновлень, що визначає можливість створення контенту всіма користувачами мережі Інтернет: в LMS створювати компоненти навчального середовища уповноважений лише викладач, який користується відповідними привілеями та правами доступу;

відсутність інтеграції зі сторонніми сервісами мережі Інтернет, у зв’язку з чим зростає кількість облікових записів у різних інформаційних системах, веб-порталах, соціальних сервісах та ін.;

складність в обслуговуванні та технічному супроводі таких систем, що потребує підтримки IT-інфраструктури ВВНЗ.

Разом з тим, останнім часом розвивається новий клас систем, що реалізують управління навчальним контентом (Learning Content Management System, LCMS). Такі системи забезпечують управління змістом навчальних програм, а не процесом навчання, і орієнтовані на розробників контенту, спеціалістів з методологічного компонування курсів та керівників проектів навчання. В основі LCMS лежить концепція представлення змісту навчання, як сукупності навчальних об’єктів, що багаторазово використовуються, зі своєю цільовою аудиторією та певним контекстом використання. На думку фахівців, межі між цими двома класами систем немає, так як більшість виробників систем LCMS забезпечують їм функції LMS.

Ринок LCMS поки ще досить фрагментований, що свідчить про його незрілість, проте швидко розвивається. Системи цього класу стають все більш затребуваними і розглядаються не просто як необхідна інфраструктура для e-learning, але, принаймні західними компаніями, і як частина загальної корпоративної IT-інфраструктури. Підтвердженням цього є інтерес, який виявляють до рішень з управління навчанням виробники систем загального управління, зокрема компанії SAP (SAP Learning Solution), Oracle (iLearning), PeopleSoft (Enterprise Learning Management).

Варто підкреслити те, що Learning Management Systems (LMS) та Learning Content Management Systems (LCMS) мають різні завдання, а саме, головне завдання LMS – автоматизувати адміністрування навчального процесу, а LCMS – управління змістом навчальних курсів.

Обидві системи LMS та LCMS керують змістом курсів та відстежують результати навчання. Обидва інструменти можуть керувати та відстежувати контент до рівня навчальних об’єктів. Але LMS, водночас, може керувати і відстежувати змішане навчання, що складається з онлайнового контенту, заходів у навчальних класах, зустрічей у віртуальних навчальних класах та інших джерел. На противагу цьому, LCMS не може керувати змішаним навчанням, зате може керувати контентом на рівні грануляції нижче за навчальний об’єкт, що дозволяє закладу більш просто здійснювати реструктуризацію та перенацілювання онлайн-контенту. Додатково, сучасні LCMS забезпечують динамічне будування навчальних об’єктів відповідно до профілів користувачів або стилів навчання [56].

При вирішенні завдань організації дистанційного навчання важливо правильно вибрати автоматизовану програму-оболонку, що дозволяє забезпечити процес функціонування системи дистанційного навчання.

На основі аналізу існуючих систем LMS/LCMS з відкритим кодом доцільно звернути увагу на такі: Moodle, ATutor, Claroline, Dokeos, LAMS, OLAT, OpenACS, Sakai [56, 141 – 145].

MOODLE (Modular Object-Oriented Dynamic Learning Environment) – це найбільш відоме середовище дистанційного навчання, яке забезпечує створення якісних дистанційних курсів. Дане ПЗ запроваджено в більш ніж у 100 країнах світу школами, університетами та викладачами. За своїми можливостям Moodle є поруч з відомими комерційними системами управління освітнім процесом, у той же час вигідно відрізняється від них тим, що поширюється у відкритих вихідних кодах – це дає можливість доповнити її новими сервісами.

ATutor є вільно розповсюджувана веборієнтована система управління навчальним контентом, яка має властивості доступності та адаптованості. Системні адміністратори мають можливість оновити або інсталювати

ATutor та створювати оригінальні шаблони оформлення системи. Викладачі та студенти працюють з адаптивним навчальним середовищем.

CLAROLINE (Classroom Online) – для розробки сайтів дистанційного навчання. Додаток створений в Інституті педагогіки та мультимедіа Левеньського католицького університету (Бельгія). Безкоштовний та може прийняти до 20 000 учнів. ПЗ дозволяє створювати заняття, редагувати їх вміст, керувати ними. Додаток включає форуми, календар, функцію розмежування доступу до документів, каталог посилань, систему контролю над успіхами учня, модуль авторизації.

DOKEOS – платформа побудови сайтів дистанційного навчання, що базується на гілці (fork) Claroline. Гілка є клоном програмного продукту, що вільно розповсюджується, створений з метою змінити додаток-оригінал у тому чи іншому напрямку. Dokeos – результат роботи деяких членів команди розробників Claroline, які задумали: змінити орієнтацію програми. Тепер вона підійде швидше організаціям, аніж університетам. Справа в тому, що Claroline чудово адаптована для університетського середовища, що виражається у підтримці великої кількості учнів та курсів. Однак, за своїм функціоналом Dokeos більше орієнтований на професійних користувачів, наприклад, на Персонал закладу.

LAMS – специфікація IMS Learning Design розроблена на основі результатів роботи Відкритого університету Нідерландів (Open University of the Netherlands – OUNL). На основі даної специфікації була створена Система управління послідовністю навчальних процесів – Learning Activity Management System (LAMS).

OLAT – розробка University of Zurich, Switzerland, в якому вона є основною освітньою платформою електронного навчання.

OpenACS (Open Architecture Community System) – ПЗ для розробки масштабованих освітніх ресурсів.

SAKAI – онлайн система для організації освітнього простору. Має повністю відкритий вихідний код, що постійно підтримується групою розробників. У систему інтегровано підтримку стандартів та специфікацій IMS Common Cartridge, SCORM.

Системи з відкритим кодом дозволяють вирішувати ті самі завдання, що й комерційні системи, але при цьому користувачі мають можливість доопрацювання та адаптації конкретної системи до своїх потреб та поточної освітньої ситуації. Більшість систем з відкритим кодом є крос-платформними рішеннями і не прив’язані ні до конкретних операційних систем, ні до конкретних Web-браузерів. Також важливим є те, що використання комерційних СДН недоступне більшості ВНЗ через їх високу вартість, необхідність продовження ліцензії на кожен навчальний рік, прив’язку вартості ліцензій та їх продовження до кількості користувачів системи.

Сучасні тенденції розвитку Open Source LMS/LCMS спрямовані у бік універсалізації та збільшення функціональності систем. За своїми можливостями найбільш просунуті системи не поступаються комерційним аналогам, а деякі навіть перевершують їх. СДН з відкритим вихідним кодом дозволяють реалізувати той самий набір функціональних можливостей, що й комерційні рішення зі значно меншими економічними витратами.

Аналіз інформаційних ресурсів Інтернету та відгуків на форумах з проблем СДН показав, що найбільший інтерес серед Open Source систем представляє Moodle. Відмінна особливість проекту Moodle полягає в тому, що навколо нього сформувалося найбільш активне міжнародне мережеве співтовариство розробників та користувачів, які діляться досвідом роботи на платформі, обговорюють проблеми, що виникають, обмінюються планами та результатами подальшого розвитку середовища.

Варто підкреслити те, що існуючі LMS/LCMS не повною мірою відповідають усім потребам суб’єктів освітнього процесу, що служить

підставою для пошуку альтернативних варіантів реалізації освітніх систем, серед яких найбільш перспективним бачиться використання інформаційних технологій, під якими розумітимемо галузь обчислювальних технологій, що забезпечують на вимогу користувача віддалений доступ до цілого набору навчальних ресурсів (додатків, сервісів, сховищ даних), розміщені на серверах в мережі Інтернет. При цьому доступ до ресурсів надається користувачам за допомогою хмарних сервісів – безкоштовних чи умовно безкоштовних хмарних програм, програмні та апаратні вимоги яких не передбачають наявності у клієнтів високопродуктивних та ресурсозалежних комп'ютерів [56].

Також важливо звернути увагу на стратегію розвитку СДН, яка повинна базуватися на активному впровадженні технологій штучного інтелекту [44, 58, 59, 66]. На даний час ШІ використовують в основному для оцінки знань та успішності слухачів. Але приклад з нейромережею Chat GPT свідчить про бурхливі результати та про те, що ймовірне очікуються її впровадження саме в LMS.

1.2. Аналіз технологій захисту персональних даних в системах дистанційного навчання

Персональні дані. Дослідження, яке проведено в межах дисертаційної роботи підтверджує актуальність тривіального твердження про важливість захисту персональних даних в інформаційних системах, а саме, в системах дистанційного навчання. Варто звернути увагу на те, що пакет нормативно-правових актів захисту даних (Загальний регламент про захист даних), прийнятий у травні 2016 року, спрямований на те, щоб зробити Європу цифровою. Загальний регламент про захист даних (англ.

General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) – регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Він також регламентує експорт персональних даних за межі ЄС і ЄЕЗ. Більше 90% європейців стверджують, що вони хочуть мати право на захист даних в ЄС незалежно від того, де їх дані обробляються. Комерційні компанії, web-ресурси, державні заклади та добровольчі організації виконують роботу з обробки та захисту персональних даних своїх клієнтів. Реєстр здійснюється з допомогою організаційних, технічних та технічних сторінок та створення необхідної документації. Однієї окремою метою дослідження даного розділу є визначення концепції персональних даних, теоретичних та юридичних аспектів їх захисту, перегляд існуючих рішень і поглядів провідних міжнародних компаній та аналіз основних положень Загального регламенту захисту даних.

Перший крок – це визначити, що є персональними даними. На основі тексту Загального Регламенту про захист даних, йдеться, що персональні дані є будь-якою інформацією, що стосується ідентифікованої фізичної особи (власника даних), яка може бути безпосередньо або опосередковано ідентифікована. Інформація, зібрана разом, може призвести до ідентифікації певної людини, а також до ідентифікації його чи її особистої інформації. Персональні дані, які були де-ідентифіковані та зашифровані але можуть бути використані для переідентифікації осіб, залишаються в публічному домені і не охоплюються законом, хоча вважаються приватною інформацією.

Анонімні дані не вважаються «персональними даними», так як особа не є або більше не може бути ідентифікована. До персональних даних відносяться [10, 20, 28, 49, 60]:

ПІБ (прізвище, ім’я, по-батькові);

домашня адреса;

адреса електронної пошти;

номер ID-картки;

будь-які дані про місцезнаходження;

адреса інтернет-протоколу (IP);

ідентифікатор cookie;

ідентифікатор реклами вашого телефону;

дані веб-портрету;

дані особи, що знаходяться в лікарні;

дані розумової, генетичної, фізичної, економічної, культурної і соціальної ідентичності особи, які дозволяють достовірно визначати цю особу.

Також існують типи даних, що класифікуються як особисті або конфіденційні персональних дані. Вони надають інформацію про:

расове або етнічне походження;

політичні погляди;

релігійні або філософські переконання особи;

членство в різних спілках.

До цієї групи відносяться біометричні (генетичні) дані, які можуть бути використані для ідентифікації особи, дані про стан здоров’я особи, відомості, що стосуються сексуального життя або орієнтації.

Не є персональними даними:

реєстраційний номер компанії;

адреса електронної пошти компанії;

анонімні дані.

Концепція персональних даних у сенсі GDPR охоплює значно більшу кількість інформації, ніж це здається на перший погляд. У контексті Регламенту завжди необхідно дотримуватися правила: у разі будь-яких

сумнівів щодо інформації, що міститься в GDPR, необхідно вважати GDPR обробкою відповідно до вимог GDPR [17].

З огляду на можливість застосування положень Загального Регламенту про захист даних до українських веб-ресурсів, необхідно прийняти ряд заходів, які можуть бути вирішальними в процесі прийняття правильного рішення. Крім того, необхідно врахувати конкретні пояснення, надані відповідними європейськими органами.

У листопаді 2018 року Європейська рада з захисту прав людини розробила публічне пояснення реалізації положень GDPR щодо принципів територіального застосування (Guidelines 3/2018 on the territorial scope of the GDP). Основна мета цього дослідження була розслідування особливостей застосування GDPR для компаній і веб-ресурсів, розташованих за межами ЄС.

Дефіцієнт міжтериторіального застосування GDPR повинен бути визначений виключно в тому контексті, що положення нового Регламенту можуть бути застосовані не тільки до об’єктів, розташованих на території ЄС або Європейського економічного простору, як це було в відповідності з вимогами Директиви 95/46/ЄС, але і до об’єктів, розташованих на території всього світу. Важливо відзначити, що коли застосовується один з вищезгаданих критеріїв, діяльність підпроекту повинна бути дуже уважно аналізована. Коли організація визнає, що вона зобов’язана діяти відповідно до вимог Регламенту, вона не повинна перебувати в значній позиції щодо оброблюваних ПДА, як у статусі процесора, так і в статусі контролера. Постачання цього Регламенту застосовуються до компанії в тій же країні, що і визначена в Регламенті, щодо кожної його ролі.

Питання про те, чи повинен представник організації бути визнаний в ЄС, залишається важливим, коли йдеться про застосування діяльності організації до критеріїв цілеспрямованого приховування. GDPR – Регламент передбачає, що він застосовується до обробки персональних даних в

контексті діяльності контролера або обробника в ЄС, незалежно від того, що здійснюється органом обробки даних в ЄС. Зважаючи на застосування GDPR через використання локальних ідентифікаційних критеріїв, також необхідно зрозуміти, як ці критерії можуть застосовуватися до українських підприємств.

Факт існування української компанії (організації) на території ЄС є фактором, що визначає зобов'язання української компанії організувати свою діяльність та діяльність, пов'язані з обробкою персональних даних, відповідно до вимог Регламенту.

Технології захисту персональних даних. Перш за все проаналізуємо Закон України «Про захист персональних даних» та відповідальність за порушення законодавства про захист персональних даних (стаття 188-39 Кодексу про адміністративні правопорушення).

Необхідно підкреслити те, що технології захисту персональних даних базуються на основних сучасних організаційних, апаратних та програмних способах, засобах та процедурах захисту інформації, які в повному обсязі опубліковані в літературі [1 – 9, 12, 16 – 21, 22, 37 – 43, 60, 127 – 139 та ін.].

Також доцільно звернути увагу на те, що технології захисту персональних даних є складовою системи кібербезпеки, яка в свою чергу є підсистемою та складовою системи інформаційної безпеки (рис. 1.1.) [63, 64, 100 – 108].

Стратегії і політики інформаційної безпеки СДН забезпечується наступними підсистемами: апаратне забезпечення, програмне забезпечення, криптографічне та математичне забезпечення, організаційне забезпечення (рис. 1.2).

В той же час арсенал моделей, методів, способів, засобів та процедур, а саме, методи і заходи протидії кіберінцидентам; методи і засоби криптографічного та технічного захисту інформації та інші використовується так званою «системою управління інформаційною

безпекою та/або кібербезпекою», яка функціонує з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки (та/або кібербезпеки) та формування відповідних протидій (рис.1.3) [26].

Рис. 1.1. Місце системи захисту персональних даних в підсистемі інформаційної та кібербезпеки системи дистанційного навчання

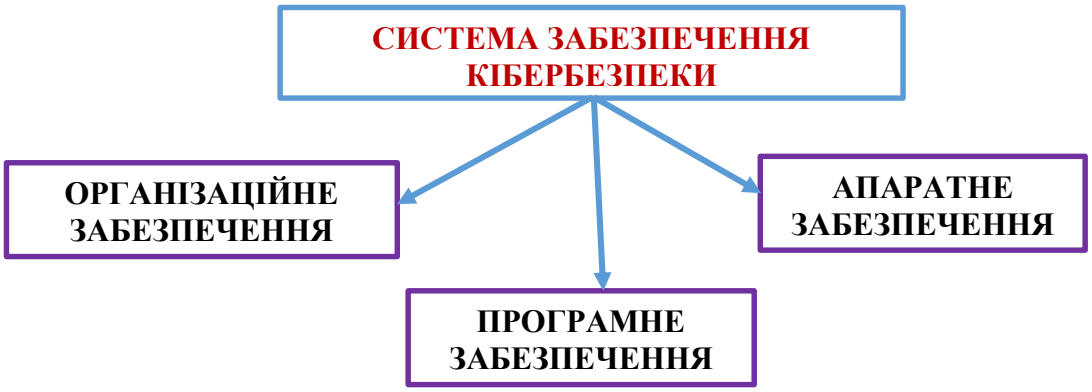


Рис. 1.2. Підсистема забезпечення кібербезпеки системи дистанційного навчання

Доцільно окремо визначити: систему управління доступом до інформаційних ресурсів; систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій в галузі інформаційної безпеки та/або кібербезпеки [31].

Система управління кібербезпекою дозволяє виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки, використовувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому (рис. 1.3) [35].

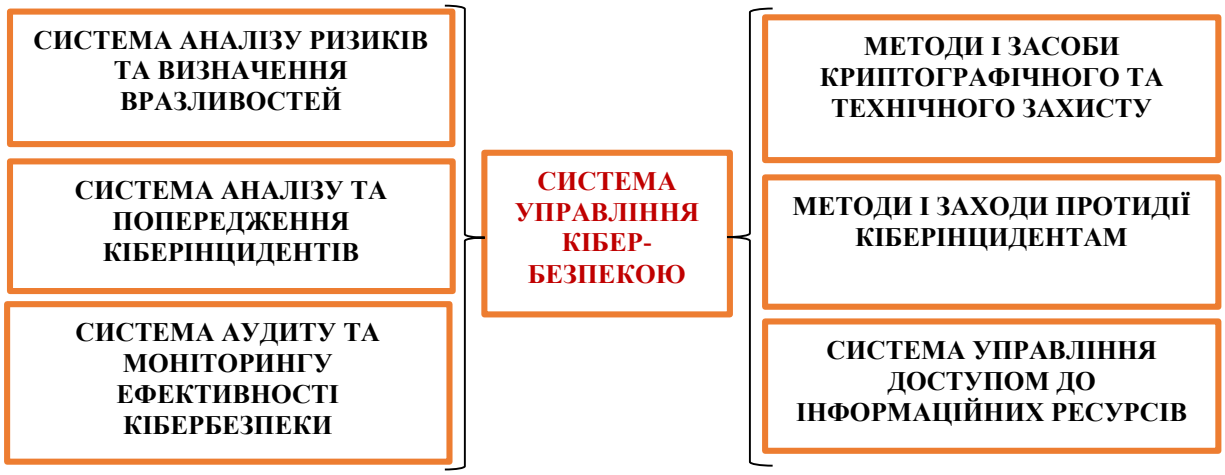


Рис. 1.3. Система управління кібербезпекою

Традиційні рішення з кібербезпеки та захисту персональних даних. Найпоширенішим захистом від кіберзагроз є безпека мережі, включаючи брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та технології шифрування. Хоча безпека мережі безумовно важлива, вона сама по собі не є рішенням проблеми захисту. На думку експертів жодна система не є на 100% безпечною, оскільки завжди

будуть уразливості, якими можуть скористатися зловмисники. Безпека мережі є одним із компонентів загальної стратегії кібербезпеки. Актуальна, так звана, хмарна безпека, яка означає захист від кіберзлочинців даних, що зберігаються в хмарних обчислювальних середовищах, таких як Amazon Web Services (AWS) або Microsoft Azure. Наприклад, безпека даних часто забезпечується шифруванням під час зберігання великих обсягів даних клієнтів у хмарному середовищі. Це можна зробити за допомогою інфраструктури відкритих ключів або еквівалентної технології [36, 44, 45].

Стратегія кібербезпеки та захисту персональних даних – це набір методів, політик і процедур, які використовуються для зменшення впливу будь-яких порушень безпеки. Він містить кроки для зниження ризику від таких загроз, як кібератаки, витоки даних і шкідливе програмне забезпечення. Стратегія кібербезпеки включає кілька компонентів: одним із компонентів стратегії кібербезпеки є оцінка ризику, яка визначає ймовірність того, що подія відбудеться, і потенційні наслідки події. Оцінка ризиків часто розглядає різні типи загроз і слабких місць у бізнесі. Наприклад, під час оцінювання можна розглянути, чи є в організації веб-сайт, який можна зламати, або чи є слабкі місця в захисті паролем. Після оцінки ризиків розробляють заходи пом’якшення, щоб зменшити ймовірність або вплив подій у сфері кібербезпеки. Заходи пом’якшення визначаються як засоби зниження ризиків подій кібербезпеки. Найпоширенішими заходами пом’якшення є контроль безпеки, шифрування та виправлення [50 – 55].

Серед численних політик є політика нульової довіри, яка є вигідною для організацій, які хочуть встановити більш надійний контроль над різними аспектами цифрової безпеки компанії. Це гарантує, що компанії можуть керувати доступом до конфіденційної інформації, переглядаючи ресурси та попередню історію користувачів. Політика нульової довіри дає

змогу зменшити ризик витоку даних і зберегти конфіденційність співробітників. Політика нульової довіри поширюється на наступне:

програми та керування даними;

зв’язок електронною поштою;

мобільні програми та програми, якими володіє або надає компанія;

хмарні обчислення, інфраструктура чи постачальники послуг зберігання чи термінали, які використовує компанія.

Політика нульової довіри корисна для організацій і співробітників, а також для конфіденційності окремих осіб. Це допомагає окремим особам створити добре захищену цифрову ідентичність і створити можливості для доступу за потреби. Політика нульової довіри – це підхід до інформаційної безпеки, згідно з яким кінцевий користувач може отримати доступ до будь-якого комп’ютера чи програми іншого користувача без жодних припущень про довіру. Політика нульової довіри, також відома як політика відсутності довіри, – це підхід до інформаційної безпеки, згідно з яким кінцевий користувач може отримати доступ до будь-якого комп’ютера чи програми іншого користувача, не створюючи довірчих відносин. Забезпечується встановлення моделі «проникнення надійних обчислень», яка вимагає від усіх користувачів і пристроїв відповідати певним вимогам перед підключенням до мережевих ресурсів. Цей термін також використовується для розуміння кібербезпеки: підхід нульової довіри був використаний для створення концепції Інтернету речей (IoT), яка спирається на обчислювальні протоколи, що не викликають довіри [77, 79, 81].

Нижче наведено стратегії захисту від кіберзагроз з огляду на звичайні заходи:

Використання брандмауера та антивірусних програм. Брандмауер – це програмне і апаратне забезпечення, яке відокремлює комп’ютерну систему від Інтернету, щоб запобігти її зараженню вірусами та іншим шкідливим програмним забезпеченням. Брандмауери діють як буфер між

зовнішнім світом і мережею і дають організаціям більший контроль над вхідним і вихідним трафіком. Подібним чином антивірусне програмне забезпечення під час запуску виявляє та блокує будь-які тривожні загрози. Цей процес часто включає сканування пристрою або мережі на наявність можливого зловмисного програмного забезпечення, а потім його видалення. Як і слід було очікувати, сучасне антивірусне програмне забезпечення може оцінювати комп'ютери з двох різних сторін. З іншого боку, це сканування системи, яке переглядає файли та запобігає будь-яким потенційним шкідливим загрозам, які можуть завдати подальшої шкоди системі. Він нічого не позбавляє, але перевіряє, що в системі немає шкідливих програм.

Комплексне сканування. За час цієї процедури переглядається кожен файл і видаляються всі можливі загрози, включаючи віруси та зловмисне програмне забезпечення. З іншого боку, це вимагає досить багато часу, оскільки потрібно переглянути всі файли та стерти їх, якщо їх визначено зловмисними, але це запобігає будь-якій потенційній шкоді в майбутньому.

Використання захищених розширень браузера. Безпечне розширення для браузера допомагає залишатися в безпеці в Інтернеті, блокуючи фішингові та шкідливі веб-сайти [92 – 94].

1.3. Постановка наукового завдання

З проведеного розгляду можна зробити висновок про те, що в сучасних умовах технології дистанційного навчання мають велике значення та продовжують розвиватися швидкими темпами. Це є актуальним і для дистанційного навчання в різноманітних навчальних закладах ЗС України [56]. Дослідження підтверджують те, що рівень ефективності, показники

якості та вартості для систем дистанційного навчання продовжують покращуватися. В той же час особлива увага повинна приділятися заходам кібербезпеки, а саме – забезпеченню захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Даний напрям розвитку відповідає міжнародним та вітчизняним вимогам. Це ще більш підкреслює актуальність наукових досліджень щодо підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України за рахунок ефективного управління існуючими способами, засобами та процедурами кібербезпеки.

На теперішній час для забезпечення гарантованого рівня захищеності персональних даних користувачів системи дистанційного навчання активно використовуються сучасні організаційні, апаратні та програмні рішення. Аналіз закордонного та вітчизняного досвіду розробки та впровадження як систем кібербезпеки взагалі, так і систем захисту персональних даних користувачів системи дистанційного навчання свідчить про можливість підвищення їх ефективності за рахунок розвитку математичного та програмного забезпечення системи управління кібербезпекою на основі машинного навчання та штучного інтелекту [44, 127 – 139 та ін.].

У минулому стратегія кібербезпеки зосереджувалася в основному на моніторингу загроз і захисті від них. Сучасна та перспективна політика та стратегія кібербезпеки спрямована на *оцінку та зменшенням ризиків*, що дозволяє уникнути фрагментів програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні, які можуть завдати шкоди. Отже, аналіз сучасного стану дає висновок про те, що перспективні стратегії кібербезпеки мають бути зосереджені на зменшенні ризиків, а не на моніторингу загроз. Ці зміни створюють абсолютно нові тенденції, які пов’язані з використанням штучного інтелекту. Природа

кібератак постійно розвивається, що вимагає розвитку відповідних методів та способів протидії. За допомогою машинного навчання штучний інтелект може скорочувати дані для швидкого аналізу та забезпечувати кібербезпеку, не забираючи багато часу, енергії та ресурсів на поточні завдання (рис.1.4).

Рис. 1.4. Постановка наукового завдання

Результати досліджень свідчать про те, що найбільш актуальним в цьому напрямку є використання моделей та методів нечіткої логіки та гібридних мереж. Стрімкий розвиток теорії нечітких множин, нечіткого виведення та нейронних мереж обґрунтовує актуальність наукового завдання удосконалення існуючого та розробки нового математичного та програмного забезпечення системи кіберзахисту персональних даних користувачів системи дистанційного навчання на основі підходів та моделей даних теорій [57].

Отже, при вирішенні проблеми забезпечення кібербезпеки системи дистанційного навчання вищих навчальних закладів ЗС України,

актуальним є *наукове завдання удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України на основі штучного інтелекту*. Вирішенню цього завдання і присвячена дана дисертаційна робота.

Висновки до розділу 1

1. Аналіз сучасного стану та перспектив розвитку систем дистанційного навчання свідчить про те, що рівень ефективності та показники ефективності системи дистанційного навчання Збройних Сил України продовжують покращуватися. Незважаючи на це, постійно виконується робота з удосконалення даної системи. Особлива увага приділяється заходам кібербезпеки інформаційних технологій, які застосовуються в системах дистанційного навчання, а саме – забезпеченню захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Дані вимоги відповідають законодавству України та Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони.

2. На підставі результатів аналізу способів, засобів та процедур кібербезпеки визначені основні підходи захисту персональних даних користувачів системи дистанційного навчання ЗС України: безпека мережі, включаючи брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та технології шифрування.

3. На думку фахівців існує тенденція постійного розвитку способів кіберзагроз та кібератак, а це в свою чергу вимагає збільшення уваги до нових розробок кібербезпеки, в тому числі для захисту персональних даних

користувачів системи дистанційного навчання ЗС України. Забезпечення високого рівня ефективності таких розробок потребує сучасних, креативних підходів, з яких найбільш доцільними є ті, які засновані на штучному інтелекті.

4. Існуюча стратегія кібербезпеки зосереджується переважно на моніторингу загроз і захисті від них. Перспективна політика та стратегія кібербезпеки мають бути спрямовані на оцінку та зменшенням ризиків, що дозволить уникнути фрагментів програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні, які можуть завдати шкоди. Отже, аналіз сучасного стану дає висновок про те, що перспективні стратегії кібербезпеки мають бути зосереджені на зменшенні ризиків, а не на моніторингу загроз. Ці зміни створюють абсолютно нові тенденції, які пов’язані з використанням штучного інтелекту.

5. Отже, при вирішенні проблеми кібербезпеки системи дистанційного навчання вищих військових навчальних закладів Збройних Сил України, актуальним є наукове завдання удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України на основі штучного інтелекту.

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

2.1. Обґрунтування впровадження штучного інтелекту в методи, засоби та процедури кібербезпеки та захисту персональних даних

В сучасних популярних та наукових публікаціях є інформація про використання штучного інтелекту в кібератаках і, безумовно, це є новою тенденцією [44, 78, 147 – 154 та ін.]. Поки що не ясно, як це вплине на майбутнє кіберзлочинності. Дослідження свідчать про те, що у кібербезпеці використовується кілька різних методів штучного інтелекту, а саме: м’які обчислення, нейронні мережі та машинне навчання. Найпоширеніші з них включають стратегії, які використовують ШІ для ідентифікації та моніторингу зловмисних дій, виявлення кіберзагроз і захисту мереж організацій. Наприклад, аналітик, який спеціалізується на зловмисному програмному забезпеченні, може використовувати алгоритми машинного навчання щоб навчити систему захисту, яка побудована на принципах штучного інтелекту, виявляти шкідливі файли або підозрілі (скомпрометовані) комп’ютери.

Система штучного інтелекту також може відстежувати поведінку окремої людини або групи, наприклад, виявляти зміни в активності в соціальних мережах або аналізувати моделі трафіку співробітників, щоб визначити тих, хто може готуватися до кіберзлочину. Під час інтеграції штучного інтелекту в кібербезпеку ключовими проблемами для організацій є те, як проєктувати та керувати даними, доступними в багатьох системах, і

як структурувати дані, щоб зробити їх доступними для когнітивних програм, які можуть включати контроль людини [78].

Разом з цією тенденцією кібербезпека також все більше використовує когнітивні технології. Когнітивні технології на основі штучного інтелекту є невід'ємною частиною цілісного підходу до кібербезпеки, в якому людський фактор керує процесом і відіграє ключову роль. Загалом кіберзахист – це простір, що постійно змінюється, де характер загроз безпеці змінюється з кожним новим кроком розвитку. Аналітики вважають, що професіонали з кібербезпеки, які можуть застосувати успішні когнітивні технології матимуть більший успіх у захисті від кібератак. Галузь також охоплює певні тенденції, які формувались роками, наприклад роль технології блокчейн, як засобу кіберзахисту та збільшення потреби в штучному інтелекті для кібербезпеки [78]. На думку фахівців прогнозується, що в результаті цих заходів ефективність IT-безпеки зросте. Кібербезпека є життєво важливою складовою будь-якого бізнесу і її може бути складно оцінити кількісно. У своєму звіті «Тенденції кібербезпеки» відома американська компанія CyberVance підкреслює важливість вивчення тенденцій стратегії кібербезпеки, зокрема, як організації можуть запровадити нові технології та захиститися від кібератак [78].

У минулому фахівці з кібербезпеки зосереджувалися в основному на моніторингу загроз і захисті від них. Тепер вони більше стурбовані оцінкою та зменшенням ризиків, що дозволяє їм уникнути експлойтів (фрагментів програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні), які можуть завдати шкоди. Аналіз сучасного стану дозволяє зробити висновок про те, що перспективні стратегії кібербезпеки зосереджені на зменшенні ризиків і оцінці ймовірності загроз, а не на моніторингу загроз (рис. 2.1).

Ці зміни створюють абсолютно нові тенденції, які пов'язані з ШІ. Більш широка класифікація методів штучного інтелекту, які

використовуються для виявлення та пом'якшення кіберзагроз, включає: експертні системи та інтелектуальні агенти.

Рис. 2.1. Перспективна стратегія кібербезпеки

Експертні системи. Експертні системи – це апаратно-програмний комп'ютерний комплекс, який надає людині право приймати рішення [91]. Системи, засновані на знаннях, складаються з двох підсистем, а саме: бази знань і механізму логічного виведення. База знань зберігає інформацію та пов'язана з механізмом виведення, який інтерпретує її або робить виведення із доступної інформації для прийняття рішень. Системи, засновані на знаннях, можуть робити прогнози та судження на основі інформації в базі знань. Їх можна використовувати в таких завданнях, як медична діагностика, біржова торгівля або навіть прогнозування майбутнього. Система, заснована на знаннях, – це комп'ютерна система, яка поєднує обчислювальний механізм (Inference Engine) і сховище даних, щоб робити прогнози щодо невідомих змінних на основі заданих відомих змінних [95]. Прикладами таких систем є Weather Channel, Google search, Alexa або Siri.

Системи, засновані на знаннях, використовують наявний масив знань для створення моделей прогнозу, які використовуються в конкретних сценаріях (рис.2.2).

Рис. 2.2. Технології штучного інтелекту в кібербезпеці

Інтелектуальні агенти. Інтелектуальний агент – це програмне забезпечення, яке існує в середовищі, яке не контролюється ніким із зовні. Він може реагувати на коливання свого оточення та постійно досягати своїх цілей протягом тривалого часу. У них завжди є кілька способів досягнення цих цілей. Інтелектуальний агент може бути розроблений таким чином, щоб вивчати всі можливі дії, а потім вибирати найкращий варіант для досягнення своєї мети. Розумні агенти – це ті, хто має здатність навчатися та адаптуватися до середовища [35].

Штучний інтелект можна використовувати для виявлення та припинення кібератак шляхом імітації людського інтелекту. Він може виявляти моделі поведінки, щоб визначити потенційні сигнали загрози, які вказують на потенційну атаку. Машинне навчання можна використовувати

в кібербезпеці для виявлення та запобігання цілеспрямованим атакам на промислові системи управління [78].

Пом'якшення кіберзагроз за допомогою штучного інтелекту.

Виявлення та ідентифікація зловмисного програмного забезпечення. Штучний інтелект, який використовується для виявлення та ідентифікації зловмисного програмного забезпечення, все ще перебуває в початковому стані, але він має потенціал кардинально змінити спосіб боротьби з кіберзлочинністю. Штучний інтелект може допомогти ідентифікувати шкідливі файли до того, як вони досягають кінцевого користувача, і, таким чином, може забезпечити значні переваги безпеки. Для виявлення зловмисного програмного забезпечення використовувалося багато різних підходів штучного інтелекту та машинного навчання, деякі з них більш успішні, ніж інші [78, 99].

Один із підходів використовує машинне навчання та інтелектуальний аналіз даних для пошуку сховищ вихідного коду зловмисного програмного забезпечення за допомогою техніки під назвою «SourceFinder» та аналізує їх на основі характеристик і властивостей [132]. Інший спосіб використовує машинне навчання для пошуку певних рядків у файлах, які можуть вказувати на наявність зловмисного програмного забезпечення або зловмисного коду, а також для їх класифікації [148]. Ще один підхід полягає у використанні штучного інтелекту та машинного навчання для виявлення шаблонів у двійкових виконуваних файлах і визначення їх шкідливості [140]. Інший метод виявлення та зупинки зловмисного програмного забезпечення полягає у використанні візуальних двійкових шаблонів, визначених у коді, і типу самоорганізованої мережі, яка адаптується з часом [84].

Системи зазвичай використовують евристику – процес пошуку закономірностей у даних – для пошуку зловмисного програмного забезпечення шляхом сканування величезних наборів даних і пошуку

підозрілих файлів, які можуть бути індикаторами наявності шкідливого програмного забезпечення. Іншими словами, системи можуть використовувати хеш-значення для виявлення файлів, які нещодавно змінено, або вони можуть використовувати показники розміру файлу протягом певного періоду часу, щоб визначити, що новий файл виглядає занадто великим. Антивірусна програма розроблена для використання евристики та може застосовувати такі методи, як зіставлення шаблонів, статистичний аналіз і емуляція відомих сигнатур зловмисного програмного забезпечення [78].

У роботі [90] представлено аналіз байтової активації на основі нейронної мережі, де відповідь на вхідний сигнал відображається на активацію кожного байту. Автор статті [109] використовував нейронну мережу Convolution, було навчено три мережі з різними параметрами, такими як розміри навчального набору та налаштування вилучення. Щоб знайти конкретні параметри, було проведено навчання мереж із певним набором даних із 7 мільйонів файлів. Змагальні приклади – це вхідні дані з невеликими, непомітними варіаціями, через які нейронні мережі змінюють їх.

Нейронні мережі, призначені для автоматичного виявлення зловмисного програмного забезпечення, можуть бути не захищені від цих типів атак, і саме вони є предметом роботи [86]. Мета цієї мережі полягає в аналізі структури для створення змагальних прикладів, які неправильно класифіковані. Подібний підхід застосовувався раніше, але результати, отримані в цьому дослідженні, відрізняються від тих, що представлені у [110] і [116]. Крім того, автори [86] доводять, що їх техніка може забезпечити краще розуміння кожної класифікації з [78, 90], а також досліджувати нові області рішень для пошуку кращої продуктивності. Архітектура включає два фільтри №1 та №2, де фільтр №1 призначений для

виявлення хорошого програмного забезпечення, а фільтр №2 призначений для пошуку певних частин у файлі, які роблять його шкідливим.

Техніка обфускації коду є проблемою для методів на основі сигнатур, які використовуються вдосконаленим зловмисним програмним забезпеченням для ухилення від інструментів захисту від зловмисного програмного забезпечення. Щоб вирішити цю проблему, автори статті [146] пропонують підхід, який вони використали для покращення точності виявлення невідомого вдосконаленого зловмисного програмного забезпечення, і запропонували новий метод, який використовує критерій Фішера для вибору функцій і п’ять класифікаторів для виявлення невідомого шкідливого програмного забезпечення.

Кілька інших відомих публікації за темою: автори [89] опублікували статтю про класифікацію та виявлення зловмисного програмного забезпечення за допомогою аналізу даних і машинного навчання. Вони використовують ці методи для класифікації шкідливих веб-сайтів, які потенційно можуть призвести до зараження. Автори статті [96] використовували стратегії алгоритмів машинного навчання KNN і SVM для виявлення невідомих шкідливих програм у даних. Виявлення зловмисного програмного забезпечення в пристроях з ОС Android досліджено в роботі [122], де використовувалася ШІ для ідентифікації шкідливого програмного забезпечення в пристроях Android, і в [158], де використовувався новий підхід – алгоритми машинного навчання ML. Автори в [156] представляють нову модель глибокого навчання, яка встановлює модель SAE для інтелектуального виявлення зловмисного програмного забезпечення, яка побудована на аналізі викликів API Windows. Експериментальні результати показують, що цей метод може запропонувати набагато більше, ніж традиційне неглибоке навчання, у виявленні зловмисного програмного забезпечення та покращити загальну продуктивність [78].

Виявлення спаму. Штучний інтелект також можна використовувати для виявлення спаму шляхом аналізу вмісту повідомлення та пошуку шаблонів, типових для спаму. Це робиться за допомогою алгоритмів машинного навчання, навчених на великій кількості прикладів спаму та інших повідомлень. У процесі виявлення спаму штучний інтелект часто замінює людину та може ідентифікувати спам, не потребуючи втручання людини. Автоматизована система також може позначати повідомлення, як потенційно існуючі:

автоматично виявляє фішингові шахрайства електронною поштою;

зберігає електронні листи зі шкідливим вмістом у папці карантину;

запускає сповіщення користувача, коли система виявляє новий вірус в електронному листі;

детальні журнали всіх дій електронної пошти;

виявляє електронні листи, які містять фішингові посилання;

автоматично створює звіт про кожну виявлену електронну пошту.

Метою системи виявлення фішингу є автоматичне виявлення електронних листів, які містять фішингові посилання, і звітування про них. Наприклад, автори статті [78] використовували нейронну мережу для виявлення фішингових веб-сайтів за допомогою алгоритму Монте-Карло та підходу до мінімізації ризиків. Інший підхід описано у [118] де автори запропонували систему виявлення фішингових веб-сайтів з використанням алгоритмів машинного навчання, яка відстежувала б різноманітні функції законних і фішингових уніфікованих локаторів ресурсів (URL). Вони мають справу з алгоритмами машинного навчання для виявлення фішингових URL-адрес і використовують методи ML для подолання недоліків методів на основі чорного списку та евристичних методів, які не можуть виявити фішингові атаки.

Система виявлення вторгнень. Використання штучного інтелекту для систем виявлення вторгнень є новою галуззю, що розвивається. Це

розділ інформатики, який займається розробкою інтелектуальних систем для виявлення, класифікації та реагування на кібератаки.

Вони призначені для виявлення зловмисної поведінки та припинення її до того, як вона спричинить будь-яку шкоду. Він може бути реалізований як окрема система або як додатковий модуль до іншого програмного забезпечення безпеки, наприклад, антивірусних програм. Система виявлення вторгнень зазвичай налаштована за допомогою набору правил, які визначають, що є атакою, наприклад, використання певних слів у темі повідомлення електронної пошти або надсилання занадто великої кількості повідомлень за певний період часу. Тоді система порівнює кожен пакет даних із цими правилами та вживає заходів, якщо є відповідність. Система виявлення вторгнень зазвичай налаштована на створення сповіщень, коли вона виявляє подію, яка може свідчити про атаку чи спробу вторгнення.

Відповіді системи можна класифікувати на два основні типи. Активний захист – це той, у якому система ініціює відповідь. Наприклад, вона може попередити черговий персонал про можливу спробу вторгнення. Активний захист є найближчим до захисту «в реальному часі», оскільки система починає дію в момент виявлення, а не чекає звіту від іншої системи. Пасивний захист – це захист, при якому система реагує лише після отримання та обробки інформації про спробу вторгнення. Прикладом такого типу реакції може бути система, яка вже встановлена на місці, відстежує зміни в мережевому трафіку навколо свого периметра, а потім ініціює звіт про ці зміни в центр моніторингу, а також зберігає дані в аналітичній базі даних.

Метою алгоритму на основі ШІ є оптимізація певних функцій і вдосконалення його класифікаторів, щоб він міг зменшити кількість помилкових тривог, які виникають під час спроби ідентифікувати зловмисника. Це також може допомогти запобігти й усунути потенційні ризики безпеки в середовищі компанії з моменту їх виявлення. Комбінацію

SVM (метод машинного навчання – метод опорних векторів) і модифікованого k-середнього використовували для створення системи виявлення вторгнень в роботі [80]. У [78] використовували нечітку логіку разом із генетичним алгоритмом для виявлення будь-якої аномалії в мережі. Це мало передбачити мережевий трафік за певний проміжок часу.

Детальний огляд зусиль з виявлення вторгнень за останні кілька десятиліть наведено в [78]; перерахувавши багато робіт, автори дійшли висновку, що методи гібридного машинного навчання широко використовуються. Автор [86] запропонував гібридну архітектуру аналізу даних аудиту та інтелектуального аналізу, де за виявленням аномалії слідує виявлення неправильного використання. У [78] покращено виявлення аномальних вторгнень за допомогою самоадаптивного алгоритму Байєса, який призначений для використання у великих обсягах даних. Інший підхід інтегрував вибір функцій на основі кореляції для вибору найкращого набору функцій. Це призвело до підвищення рівня виявлення скороченого набору даних, оскільки було обрано найкращий набір функцій і видалено неважливі набори даних [78]. Було запропоновано нову методику зменшення розмірності даних [117]. Замість використання традиційної нейронної мережі автори використовують трикутний підхід для обчислення та візуалізації даних.

Отже, моделі та методи штучного інтелекту можуть виявляти та зупиняти кіберзагрози в реальному часі з обмеженими ресурсами (рис. 2.3).

Природа кібератак, що постійно розвивається, означає, що фахівцям доведеться намагатися не відставати від кіберзлочинців. Однак за допомогою машинного навчання штучний інтелект може скорочувати дані для швидкого аналізу та забезпечувати відмінне покриття безпеки, не забираючи багато часу чи енергії на поточні завдання. Машинне навчання дозволяє аналітикам зосередитися на інтерпретації результатів глибокого аналізу та розробці нових методів боротьби з кіберзлочинністю.

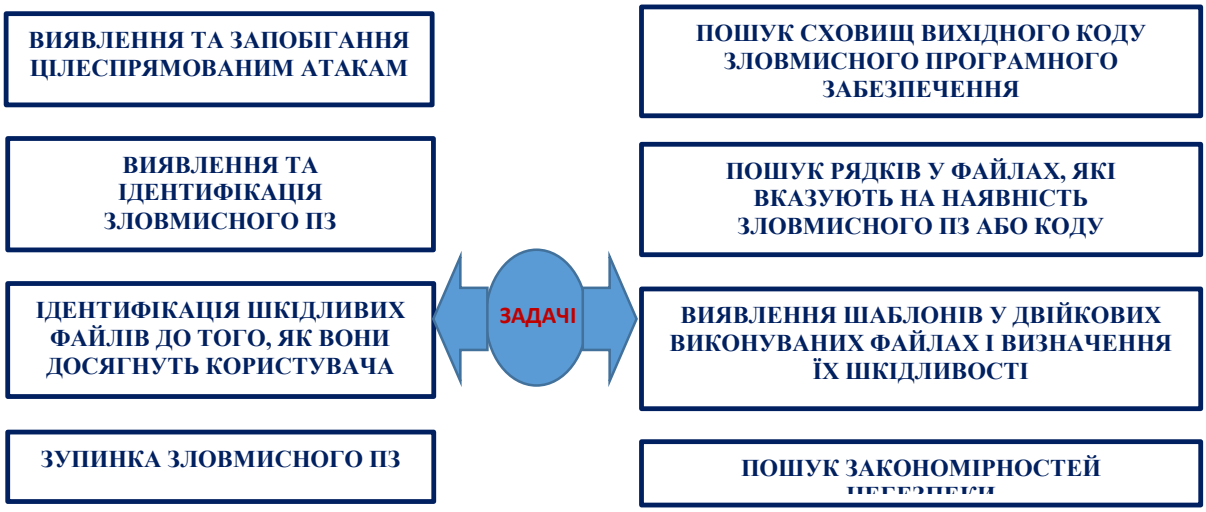


Рис. 2.3. Задачі кібербезпеки, які вирішує штучний інтелект

Варто підкреслити те, що технології ШІ не є високоефективними для всіх форм кібербезпеки. Але підходи на основі штучного інтелекту стають все більш поширеними та економічно ефективними в більшості аспектів кібербезпеки. Дослідження показують, що штучний інтелект позитивно вплинув на кібербезпеку та ризики. Отже, продовження впровадження штучного інтелекту та машинного навчання виведе сферу кібербезпеки на новий рівень інтелекту [97, 113–115].

2.2. Обґрунтування концепції підвищення захищеності персональних даних на основі штучного інтелекту

Отже, як видно з попереднього розгляду, перспективні стратегії кібербезпеки будуть зосереджені на зменшенні ризиків, а їх теоретичним підґрунтям є штучний інтелект. В даній дисертаційній роботі математичні моделі та методи розроблені для підвищення захищеності персональних

даних користувачів системи дистанційного навчання ЗС України і базуються на методах нечіткої логіки та гібридних мережах. Дана концепція включає наступні ключові компоненти [57], які будуть описані нижче в цьому розділі.

Апарат математичної логіки для розробки адекватної та ефективної моделі прийняття рішення при підвищенні захищеності персональних даних СДН ЗС України. Використання детермінованих або стохастичних залежностей та відповідних алгоритмів для забезпечення підвищення захищеності персональних даних викликає певні труднощі, які, перш за все, пов'язані з неадекватністю, неповнотою або відсутністю необхідних даних для створення аналітичних виразів. В такому випадку адекватним є апарат математичної логіки, а саме, алгебри логіки – її розділу, який дозволяє формально визначати систему логічних операцій над висловлюваннями та дати оцінку істинності цих висловлювань в бінарному вигляді. Для кібербезпеки саме висловлювання є описом стратегії та політики, її способів, методів та процедур або їх складових. Операції булевої алгебри (диз'юнкція, кон'юнкція та заперечення) розширюють можливості мультиплексних та адитивних операції. Формально даний математичний апарат оцінює висловлювання як хибне, або навпаки – істинне.

Нечіткі множини для розширення можливостей класичної (чіткої) математичної логіки. Як відомо, будь-яка математична модель має певні обмеження щодо її застосування. Бінарна оцінка висловлювання – це також обмеження. Ідея застосування нечітких множин заміняє бінарну оцінку 0 або 1 оцінкою на інтервалі [0,1].

Нечітке логічне виведення для отримання адекватної та ефективної моделі прийняття рішення при підвищенні захищеності персональних даних. Класичні моделі та методи числення предикатів першого порядку, правила виведення числення висловлювань та

продукційних систем виведення є основою так званого нечіткого логічного виведення для отримання адекватної та ефективної моделі прийняття рішення при підвищенні захищеності персональних даних.

Адаптивні нечіткі нейронні мережі (гібридні мережі) для прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз. Основна ідея гібридних мереж полягає в тому, щоб використовувати існуючу вибірку даних для визначення параметрів функцій належності, які найкраще відповідають деякій системі нечіткого виведення. При цьому для знаходження параметрів функцій належності використовуються відомі процедури навчання нейронних мереж. Наприклад, у пакеті Fuzzy Logic Toolbox системи MATLAB гібридні мережі реалізовані у формі адаптивної системи нейро-нечіткого виведення ANFIS. Гібридна мережа ANFIS являє собою нейронну мережу *з єдиним виходом і декількома входами*, що являють собою нечіткі лінгвістичні змінні. Варто підкреслити те, що терми вхідних лінгвістичних змінних описуються «вбудованими» в MATLAB функціями належності, а терми вихідної змінної представляються лінійною чи постійною функцією належності. З іншого боку, гібридна мережа ANFIS це система нечіткого виведення (алгоритм Сугено) нульового чи першого порядку, у якій кожне з правил нечітких продукцій має постійну вагу $w_{ij} = 1$ [23].

2.3. Розробка методики підвищення захищеності персональних даних на основі моделей та методів нечіткої логіки та гібридних мереж

Дослідження свідчать, що при розробці концепції підвищення захищеності персональних даних користувачів СДН ЗС України доцільно

використовувати теоретичний підхід, який спрямований на керування рівнем захищеності на основі нечіткої логіки або, так званих, систем нечіткого виведення. Отже, одним з основних напрямів використання систем нечіткого виведення є розв'язання задач керування [14, 25]. Під системою керування захищеністю персональних даних будемо розуміти з'єднання N елементів $e=\overline{1,N}$ виду (рис. 2.4) в єдину конфігурацію, яка забезпечує їм необхідну поведінку для досягнення поставленої цілі.

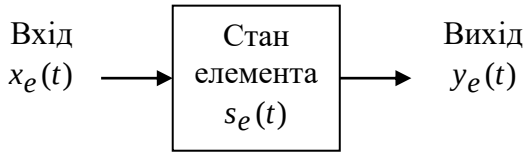


Рис. 2.4. Функціональний блок системи керування захищеністю персональних даних СДН

Зв'язок між входом (вектор-функцією $x_e(t)$) і виходом (вектор-функцією $y_e(t)$) в елементі системи (функціональному блоці) – це перетворення одного сигналу (причини) в інший (наслідок). Вся система керування захищеністю персональних даних теж може бути подана аналогічною схемою (рис.2.5).

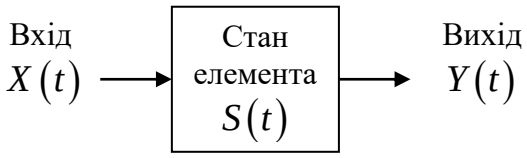


Рис. 2.5. Загальна схема системи керування захищеністю персональних даних СДН

Як відомо, системи керування поділяють на розімкнені і замкнені [25]. В розімкненій системі існує елемент – виконуючий пристрій, який визначає необхідне значення вхідного сигналу *X(t)* («приймає рішення» про необхідний вплив на систему) в залежності від бажаного (необхідного) значення виходу Y^0 (рис. 2.6).

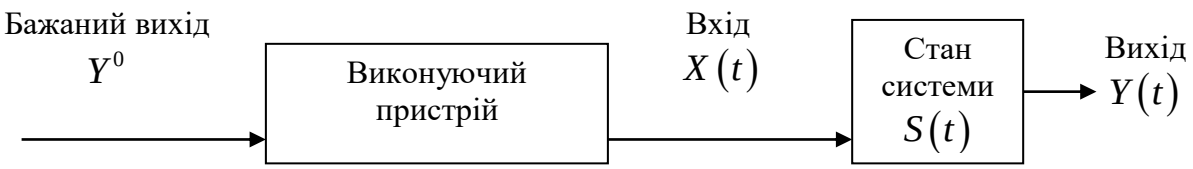


Рис. 2.6. Загальна схема розімкнутої системи керування

В системі керування елемент, який приймає рішення називають активним. Якщо система представляє собою конфігурацію активних елементів, її називають організаційною системою управління. Тоді в систему може входити елемент – координатор, який визначає вхідні сигнали активних елементів.

В замкненій системі існує зворотній зв'язок. Окремі елементи вхідного вектора *X(t)*, які можна назвати керуючими змінними, залежать від різниці між бажаним значенням вихідних величин і їх реальним значенням $Y^0 - Y(t)$ (негативний зворотній зв'язок) або від суми цих значень $Y^0 + Y(t)$ (позитивний зворотній зв'язок, рис. 2.7).

Під керуванням системою розуміють таке визначення вхідного сигналу *X(t)*, яке формує необхідну поведінку (зміну станів *S(t)*) системи для досягнення бажаних значень Y^0. Побудова нечіткої моделі системи керування базується на формальному представленні характеристик об'єкту в термінах лінгвістичних змінних [15].

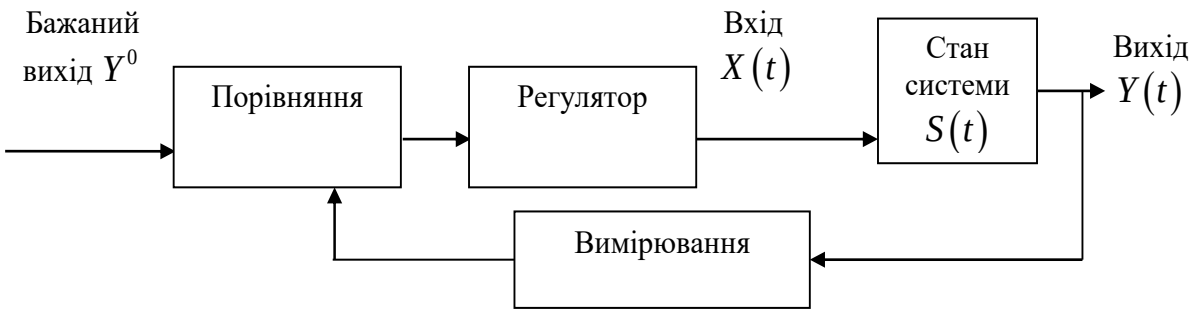


Рис. 2.7. Система керування зі зворотнім зв'язком

В системі керування в якості лінгвістичних змінних розглядаються змінні входу і виходу системи. Ціль керування полягає у визначенні значень керуючих змінних (вхідних) змінних, реалізація яких забезпечує бажану поведінку чи бажаний стан об'єкта керування. Вихідні змінні можуть знову поступати на вхід системи, утворюючи зворотній зв'язок, як показано на рис. 2.8.

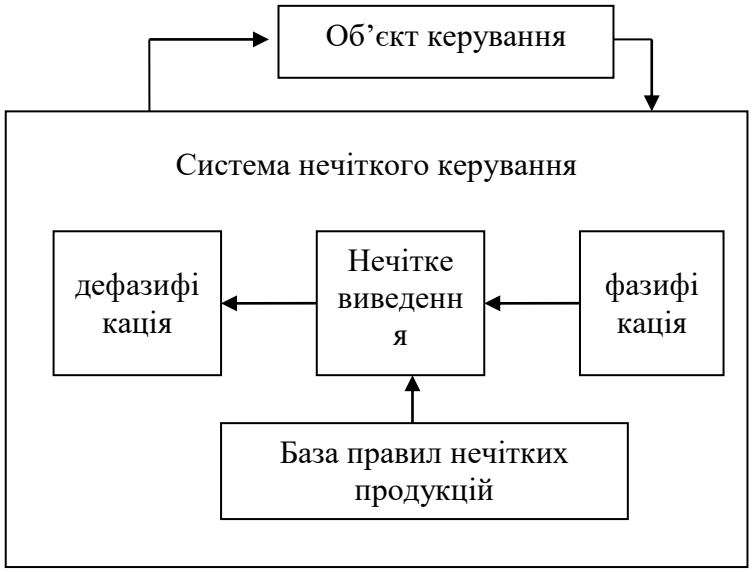


Рис. 2.8. Архітектура компонентів процесу нечіткого керування

Отже, нечітка модель системи керування захищеністю персональних даних СДН може бути описана за допомогою апарату системи нечіткого виведення.

Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України забезпечує ефективне реагування на потік загроз та базується на основі впровадження моделей та методів нечіткої логіки та гібридних мереж. Схема методики представлена на рис. 2.9.

Рис. 2.9. Методика підвищення захищеності персональних даних СДН ЗС України на основі моделей та методів нечіткої логіки та гібридних мереж

Методика поєднує моделі та методи, які спрямовані на комплексне вирішення наступних завдань:

1) ідентифікація загрози;

2) визначення стану системи захисту персональних даних, а саме, система забезпечує захист в повному обсязі або не забезпечує захист та

вимагає пошуку або розробки нових способів, засобів та процедур, які раніше не були використані;

3) формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або у випадку їх низької ефективності формування стратегії удосконалення та розробки нових;

4) прогнозування стану системи захисту в майбутньому з метою попередження шкідливого впливу загроз [57].

2.4. Розробка моделі системи захисту персональних даних

Процедура оцінки стану системи захисту персональних даних користувачів системи дистанційного навчання ЗС України є важливим етапом запропонованої в роботі, в якості наукового результату, методики підвищення захищеності персональних даних СДН. Дослідження існуючого науково-методичного апарату розробки моделей даного класу дозволило зробити висновок щодо доцільності використання нечітких алгоритмів, а саме, алгоритму Мамдані [18, 29 – 33, 119]. Даний алгоритм є прикладом так званих систем нечіткого виведення, які в свою чергу займають вагоме місце в нечіткій логіці та моделях штучного інтелекту. Процес нечіткого виведення являє собою процедуру отримання нечітких висновків на основі нечітких умов і передумов. Цей процес базується на теорії нечітких множин, а саме, на понятті лінгвістичної змінної, функції належності, нечітких імплікації та композиції. Варто підкреслити, що дана система нечіткого виведення класифікується, як продукційна нечітка система, тобто, система нечітких правил продукцій, у яких умови та результати виконання окремих правил формулюються у формі нечітких висловлювань щодо значень тих чи інших лінгвістичних змінних.

Постановка задачі. За допомогою системи нечіткого виведення на основі алгоритму Мамдані побудувати модель оцінки рівня захищеності для подальшого формування заходів щодо підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України. В моделі забезпечити метод дефазифікації з мінімальною нев'язкою, раціональну кількість правил, оптимальну вагу правил та оптимальні параметри функцій належності [57].

Оцінка стану системи захисту. Обґрунтування вхідних та вихідних лінгвістичних змінних. Опишемо та обґрунтуємо одну вихідну та 3 вхідні лінгвістичні змінні, а саме, ефективність захищеності (висока, середня, низька) залежить від: 1) ступеня навчання співробітників заходам кібербезпеки (висока, середня, низька); 2) часу, який минув після останніх заходів щодо підвищення захищеності персональних даних (мало, багато, дуже багато); 3) оцінки співробітниками існуючого рівня захищеності (високий, середній, низький).

Встановимо:

Лінгвістична змінна – це кортеж значень $\langle \beta, T, X, G, M \rangle$, де:

β– ім'я змінної (наприклад, «ефективність захищеності системи захисту»);

T – базова множина значень її термів – значень, кожне з яких надається за допомогою нечіткої множини (наприклад, «мала», «середня», «висока», «дуже висока»);

X – множина-носій можливих конкретних значень змінної для всіх термів (наприклад, $X \in [0, 100]$ балів при оцінці захищеності);

G – деяка специфічна процедура формування нових термів з множини T (наприклад, «дуже мала»);

M – семантична процедура надання терму певної нечіткої змінної вигляду$\langle X, \mu_i(X) \rangle$, $\mu_i(X)$ – функція належності i-того терму з множини T [18, 120].

Отже, **вхідні лінгвістичні змінні** та відповідні терми:

β_1– ступінь навчання співробітників заходам кібербезпеки.

T_1 = {«висока», «середня», «низька»}, в моделі позначено, як EmpTraining = {H, M, L}. Визначається в діапазоні [0, 100]. Значення показника тим більше, чим складнішим є завдання.

β_2– час, який минув після останніх заходів щодо підвищення захищеності персональних даних.

T_2 = {«дуже багато», «багато», «мало»}, в моделі позначено, як SecurityUpdateFrequency = {H, M, L}. Визначається в діапазоні [0, 100]. Значення показника тим більше, чим більшим є час.

β_3– інтегральна оцінка співробітниками існуючого рівня захищеності.

T_3 = {«низька», «середня», «висока»}, в моделі позначено, як InformationAvailability = {L, M, H}. Визначається в діапазоні [0, 100]. Значення показника тим більше, чим більша оцінка.

Вихідна лінгвістична змінна та її терми:

β_4– ефективність захищеності.

T_4 = {«мала», «не дуже мала», «середня», «не дуже висока», «висока»}, в моделі позначено, як ProtectionLevel = {L, LA, M, HA, H}. Визначається в діапазоні [0, 1] (рис. 2.10).

Обрання методу дефазифікації з мінімальною нев'язкою. Для дослідження залежності нев'язки від методу дефазифікації використана технологія порівняння експериментальних значень зі значеннями, які отримані на основі моделі алгоритму Мамдані [76].

На думку 1-ої групи експертів аналітичний вираз залежності ефективності системи захисту від 3-х чинників має вигляд

$$y = x_1^2 x_2^2 x_3, \tag{2.1}$$

на множині $x_1 \in [0,1]$; $x_2 \in [0,1]$; $x_3 \in [0,1]$.

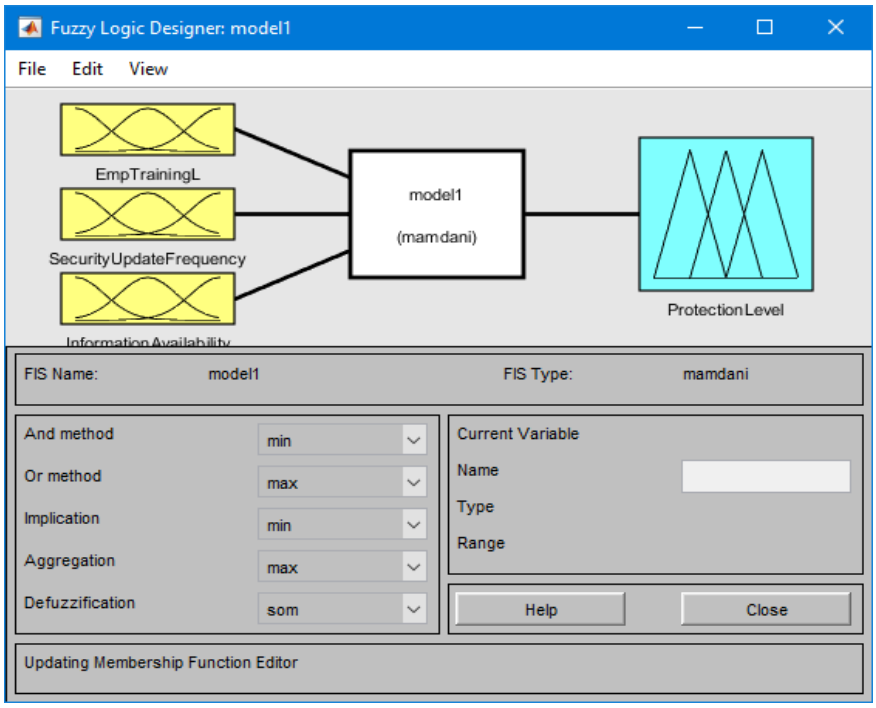


Рис. 2.10. Інтерфейс моделі

Програма візуалізації даної функції має вигляд:

```
%Побудова графіка функції y=(x1^2)*(x2^2)*x3
%в області x1є[0,1]; x2є[0,1]; x3є[0,1]
n=15;
x1=0:1/(n-1):1;
x2=0:1/(n-1):1;
y=zeros(n,n);
for j=1:n
y(j,:)=(x1.^2)*(x2(j) ^2)*0.75;
end
surf(x1,x2,y)
xlabel('x1');ylabel('x2')
zlabel('y')
title('Безпека x3=0,75')
```

Результати візуалізації для різних значень x_3 наведені на рис. 2.11.

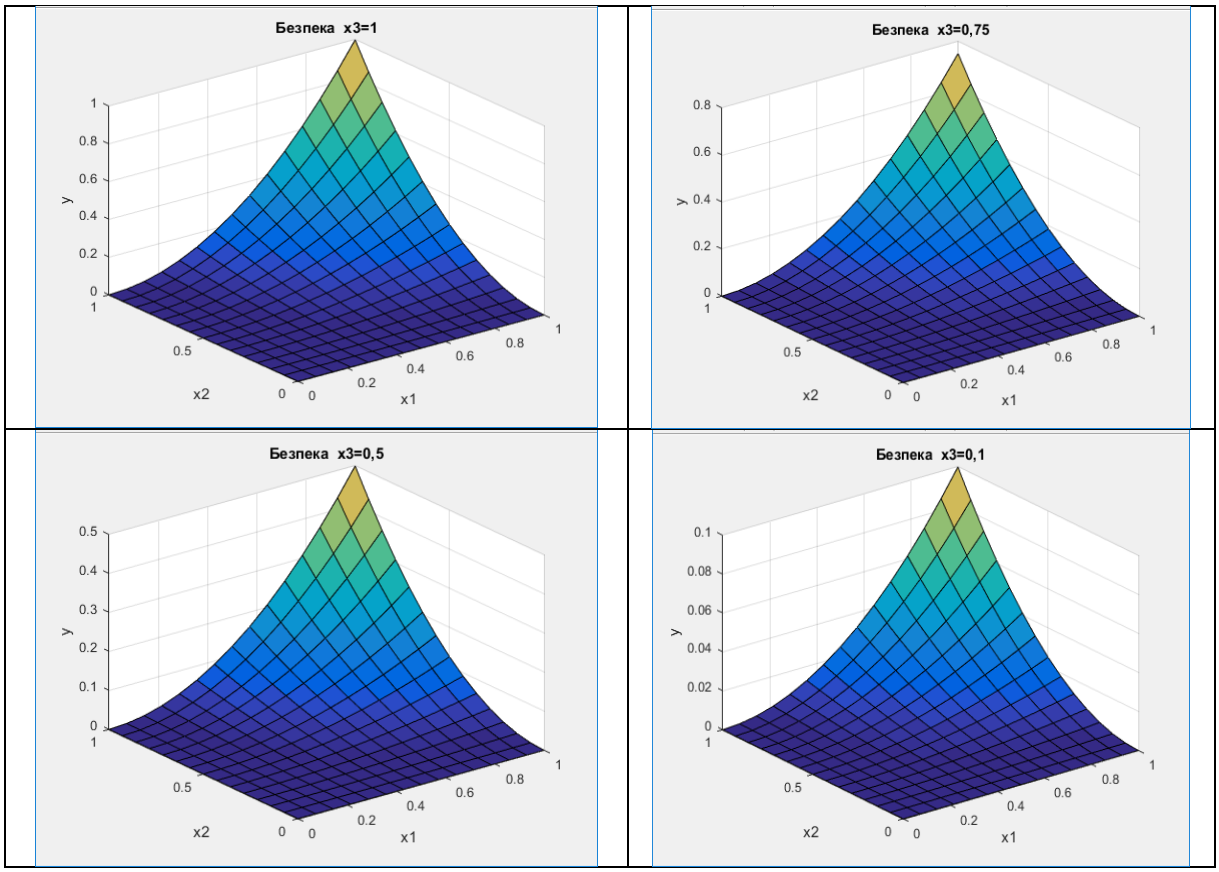


Рис. 2.11. Візуалізація $y = x_1^2 x_2^2 x_3$ на множині $x_1 \in [0,1]$; $x_2 \in [0,1]$; $x_3 \in [0,1]$ при $x_3 = 1; 0{,}1; 0{,}5; 0{,}75$

Базу правил створено шляхом візуального аналізу результатів моделювання. Розроблено програму, яка дозволяє розраховувати нев'язку для різних методів дефазифікації. Фрагмент програми для методу Centroid наведено нижче:

```
%Розрахунок нев'язки
%Генерування експериментальних точок inp та out:
n=10;
a=-7:10/(n-1):3;
b=-4.4:6.1/(n-1):1.7;
inp=zeros(n*n,2);
out=zeros(n*n,1);
l=1;
for i=1:n
```

```
     for j=1:n
inp(l,1)=a(i);
inp(l,2)=b(j);
out(l)=a(i)^2*sin(b(j)-1);
l=l+1; end
     end
%Зчитування системи нечіткого логічного висновку ql1:
ff=readfis('ql1');
%Встановлення методу дефазифікації Centroid:
ff=setfis(ff,'DefuzzMethod','centroid');
%Нечіткий логічний висновок:
outff=evalfis(inp,ff);
%Розрахунок середньої абсолютної нев'язки:
sum(abs(outff-out))/(n*n)
```

Результати моделювання представлені в табл. 2.1 та 2.2.

Таблиця 2.1

Залежність нев'язки від методу дефазифікації

Методи дефазифікації	**Середня абсолютна нев'язка**
mom	0,3429
bisector	0,3621
lom	**0,1809**
som	0,2062

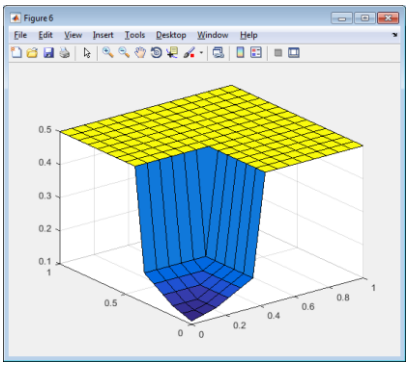
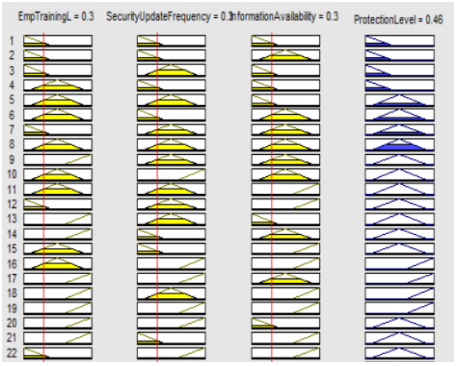
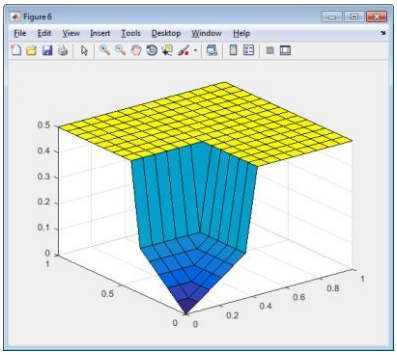
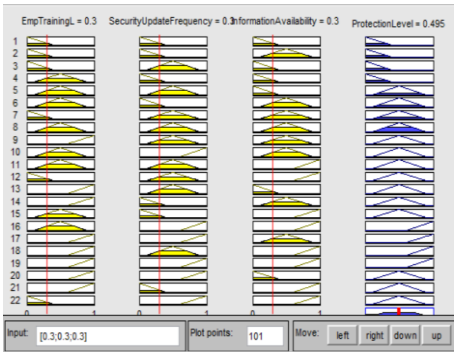
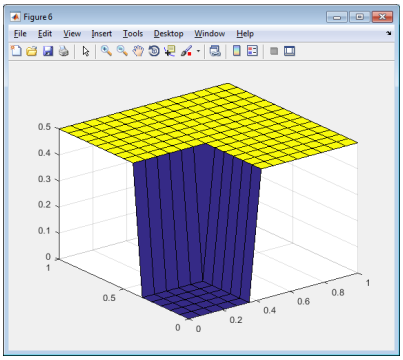
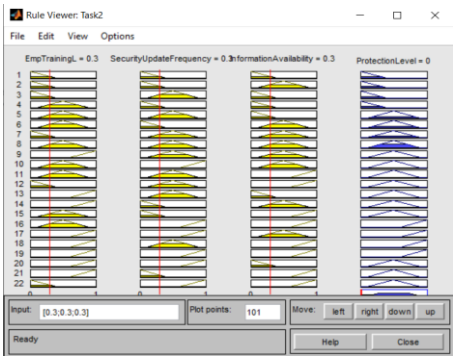
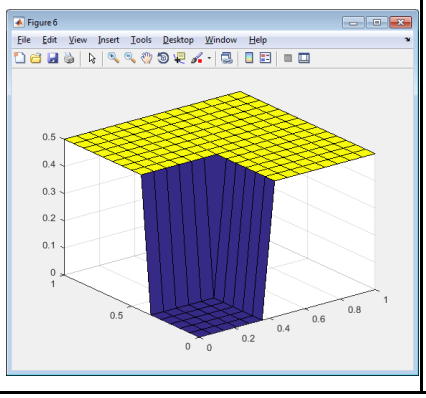
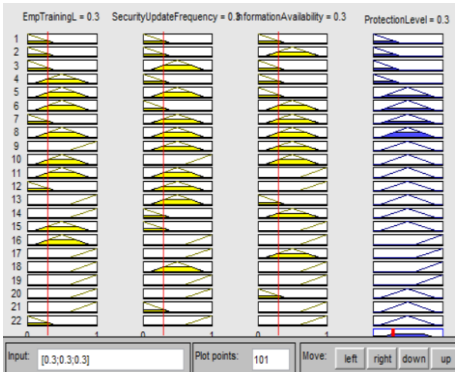
Друга група експертів на відміну від (2.1) обрала наступну аналітичну залежність ефективності від чинників

$$y = x_1 x_2 x_3, \tag{2.2}$$

на множині $x_1 \in [0,1]$; $x_2 \in [0,1]$; $x_3 \in [0,1]$.

Таблиця 2.2

Поверхні нев’язок для різних методів дефазифікації

Метод дефазифікації	Поверхня	Правила
bisector		
mom		
lom		
som		

Результати моделювання представлені в табл. 2.3 та 2.4.

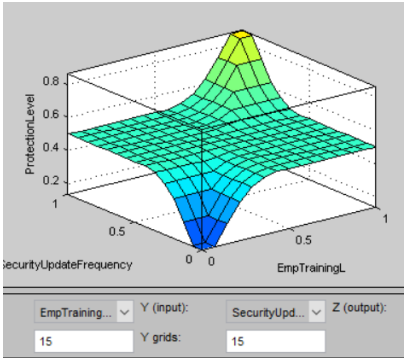
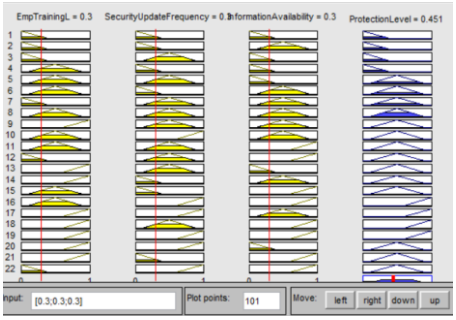
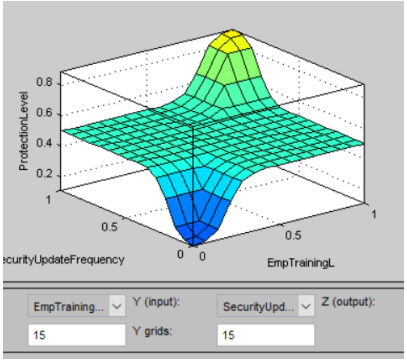
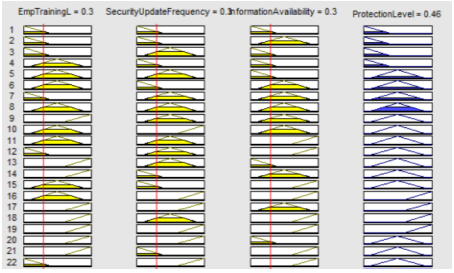
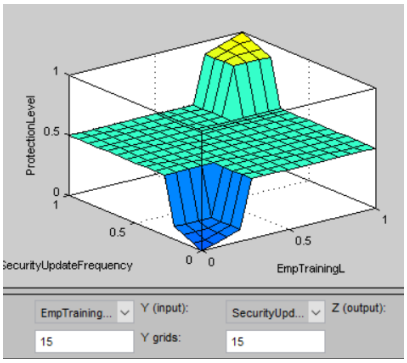
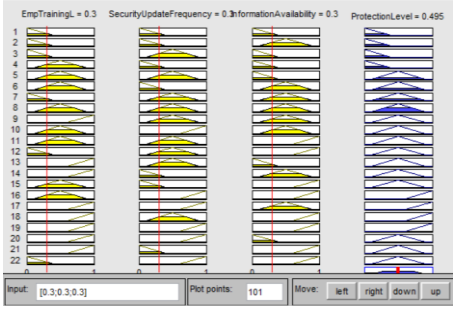
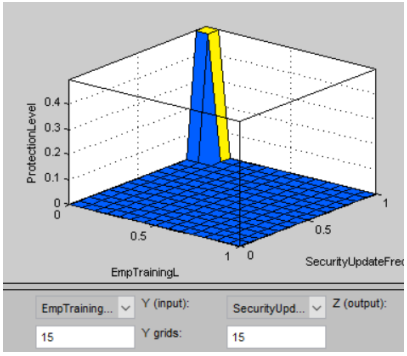
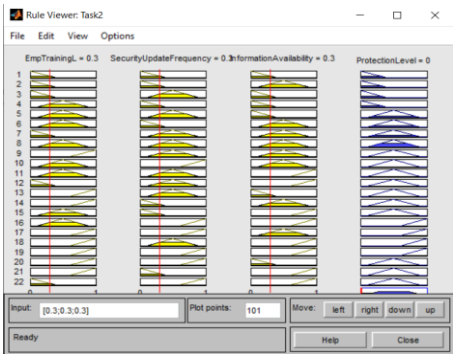
Код для розрахунку нев’язки:

```
n=11;
a=0:1/(n-1):1;
b=0:1/(n-1):1;
c=0:1/(n-1):1;
inp=zeros(n*n,3);
out=zeros(n*n,1);
l=1;
for i=1:n
     for j=1:n
          for k=1:n
inp(l,1)=a(i);
inp(l,2)=b(j);
inp(l,3)=c(k);
out(l)=a(i)*b(j)*c(k);
l=l+1;
end
     end
          end
%Зчитування системи нечіткого логічного висновку ql1:
ff=readfis('Task1');
%Нечіткий логічний висновок:
outff=evalfis(inp,ff);
%Розрахунок середньої абсолютної нев’язки:
sum(abs(outff-out))/(n*n*n)
```

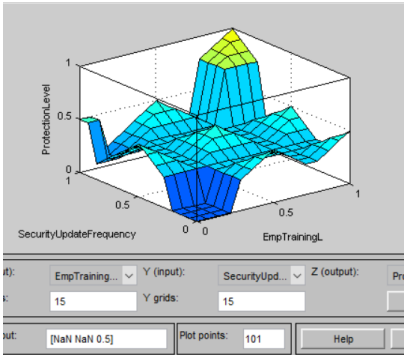
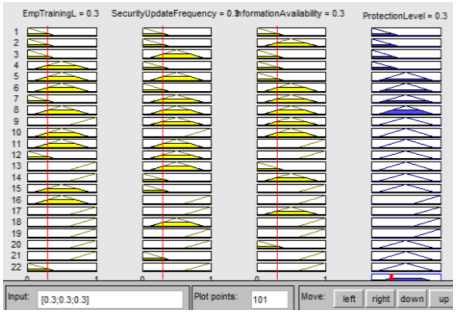
Отже, з метою мінімізації середньої абсолютної нев’язки в моделі доцільно використати метод «som» – метод лівого модального значення [23, 79 та ін.].

Таблиця 2.3

Поверхні нев’язок для різних методів дефазифікації
(при x_1 = 0.3; x_2 = 0.3; x_3 = 0.3)

Метод дефазифікації	**Поверхня**	**Правила**
centroid		 **ProtectionLevel = 0.451**
bisector		 **ProtectionLevel = 0.46**
mom		 **ProtectionLevel = 0.495**
lom		 **ProtectionLevel = 0.0**

Продовження Таблиці 2.3

som		 **ProtectionLevel = 0.3**

Таблиця 2.4.

Залежність нев’язкі від методу дефазифікації ($y = x_1 x_2 x_3$)

Методи дефазифікації	**Середня абсолютна нев’язка**
centroid	0.3707
bisector	0.3702
mom	0.3709
lom	0.4178
som	**0.2281**

Визначення раціональної кількості правил. Для розробленої раніше моделі встановлено метод дефазифікації som, так як він є найкращим і гарантує найменшу абсолютну нев’язку. Варто нагадати про те, що максимальна кількість правил в нечіткій базі знань дорівнює [121]

$$N_{max} = l_1 \cdot l_2 \cdot l_n,$$

де: l_i – кількість термів для оцінки i-ої вхідної змінної ($i = 1, \ldots, n$);

n – кількість вхідних змінних.

Також відомо про те, що однією з переваг систем нечіткого логічного виведення є їх досить ефективна робота при, так званій, «раціональній» кількості правил в базі знань, яка менша $N_{\max}$. Звичайно, збільшення

кількості правил покращує якість роботи системи, але в реальних умовах кількість достовірної інформації для їх формування може бути відсутня. Крім того, актуальною залишається відома властивість залежності «ефективність – вартість», так звана, насиченість, суть якої полягає в тому, що, починаючи з певного значення кількості правил, додавання нового правила суттєво не покращує характеристики системи виведення.

На першому інтуїтивному формуванні 22 правил середня абсолютна нев'язка дорівнює **0,2281**. Далі в базі знань була залишена мінімальна кількість правил – 3. Обчислена нев'язка – **0,3078**. Отже, нев'язка зросла на **34,9%**. Алгоритм експерименту полягає в послідовному додаванні по 3 правила поки кількість правил не стане максимальною – 27. Результати представлені в табл. 2.5.

Таблиця 2.5

Залежність нев'язкі від кількості правил

Кількість правил	**Середня абсолютна нев'язка**
3	0,3320
6	0,2762
9	0,2358
12	0,1818
15	0,1889
18	0,1865
21	0,1753
24	0,1456
27	0,1287

На рис. 2.12 наведена «крива навчання» – залежність нев'язки від кількості правил.

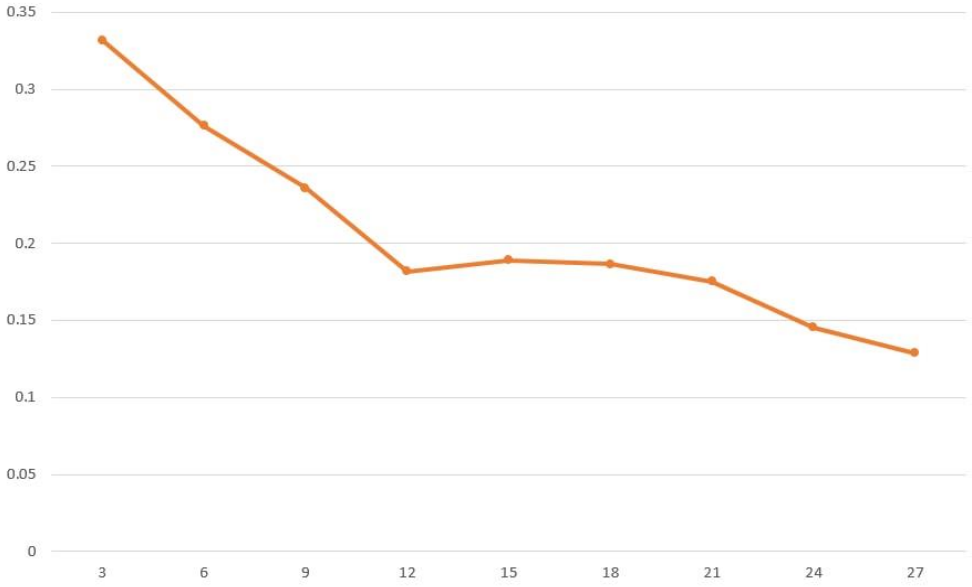


Рис. 2.12. Залежність нев’язки від кількості правил

Абсолютна нев’язка для системи з 24 правил дорівнює 0,1199. Результати дослідження для такої системи в залежності від методу дефазифікації представлені в табл. 2.6.

Таблиця 2.6

Залежність нев’язкі від методу дефазифікації для системи з 24 правил

Метод дефазифікації	**Нев’язка**
centroid	0.2165
bisector	0.2126
mom	0.2043
lom	0.1325
som	0.1199

Отже, метод лівого модального значення – «som» є найкращим методом дефазифікації при раціональній кількості правил 24. Важливим висновком є те, що збільшення кількості правил, починаючи з 12, не дає

значного приросту ефективності, тому, у випадку відсутності достовірної інформації для формування правил логічного виведення дана кількість є досить раціональною.

Формування раціональної ваги правил. Ваговий коефіцієнт продукційного правила бази знань є число в діапазоні [0,1], якому відповідає ранг даного правила в процесі формування рішення [11]. Чим більше значення вагового коефіцієнта, тим важливіше відповідне правило, і тим якісніше воно описує реальний об’єкт. В пакеті Matlab значення вагового коефіцієнта задається в дужках в кінці кожного правила. Вагові коефіцієнти правил впливають на результат нечіткого логічного виведення. В зв’язку з цим виникає задача підбору таких значень вагових коефіцієнтів правил, які забезпечують найкращу якість нечіткої бази знань. Якість нечіткої бази знань можна оцінити шляхом обчислення нев’язки між експериментальними даними та результатом нечіткого логічного висновку [111]. Підбір вагових коефіцієнтів вирішується шляхом розв’язання відповідної задачі оптимізації. Цільовою функцією цієї задачі оптимізації є якість нечіткої бази знань, а керованими змінними є вагові коефіцієнти правил. Поставлена задача являє собою багатокритеріальну задачу оптимізації.

Встановимо наступні вимоги, умови та обмеження дослідження:

1. База знань повинна складатися з не менш ніж 12 правил.

2. Критерієм якості нечіткої бази знань будемо вважати середню квадратичну нев’язку між експериментальними даними та результатами нечіткого логічного виведення.

3. Нев’язку будемо визначати для 50 експериментальних точок.

4. Експериментальні дані будемо генерувати на основі з заданої аналітичної залежності (2.2).

5. Для розв’язання задачі оптимізації будемо використовувати функції бібліотеки Optimization.

6. Завдання – перевірити роботу оптимізованої системи на вибірці з 1000 експериментальних точок.

Результати дослідження. Введемо функцію `setwrules`, яка дозволяє програмно встановлювати вагові коефіцієнти правил. Дана функція Повертає систему нечіткого висновку (`out`), яка відрізняється від початкової (`fis`) новими значеннями вагових коефіцієнтів. Вагові коефіцієнти задаються вектором `w`. Номер першого правила, для якого змінюється ваговий коефіцієнт, задається `num`. Вагові коефіцієнти змінюються для правил з номерами від `num` до `length(w)`. Якщо змінна `num` не задана, тоді вважається, що `num = 1`. Лістинг функції `setwrules`:

```
function out=setwrules(fis,w,num)
out=fis;
if nargin == 2 num=1; elseif num<1
error('Правильно задайте номер 1-го правила)end
for i=1: length(w)
out.rule(i+num-1).weight=w(i);
end
```

Далі виконується розрахунок цільової функції. Лістинг програми для розрахунку цільової функції:

```
function delta=obfunw(x)
global FIS INP OUT_AN NUM
FIS=setwrules(FIS,x);
out_fis=evalfis(INP,FIS);
delta=sum((OUT_AN-out_fis).^2)/NUM;
```

В програмі наступні позначення: `obfunw` розраховує значення цільової функції; `x` – вектор вагових коефіцієнтів правил (вектор керованих змінних; `delta` – середня квадратична нев'язка (значення цільової функції); `FIS` – система нечіткого логічного виведення; `INP` та

OUT_AN – експериментальні точки; NUM – кількість експериментальних точок.

Алгоритм оптимізації використовує функцію constr бібліотеки Optimization Matlab. Виконується оптимізація нечіткої бази знань шляхом зміни вагових коефіцієнтів правил. Код програми:

```
global FIS INP OUT_AN NUM
FIS=readfis('FuzSysName');
INP=dlmread('inp.dat',' ');
OUT_AN=dlmread('out.dat',' '); s1=size(INP);
s2=size(OUT_AN);
if s1(1)==s2(1) NUM=s1(1);
else
error('Неоднакова кількість даних INP та OUT_AN')
end
numrule=length(FIS.rule);
funf='f=obfunw(x);';
vlb(1:numrule)=0;
vub(1:numrule)=1;
options(1)=1;
x0(1:numrule)=.5;
[x,options]=constr(fun,x0,options,vlb,vub);
x options(8)
```

Обрана система нечіткого логічного виведення з 23 правил. При зміні діапазону вихідної змінної від 0 до 1, середня квадратична нев'язка буде лише зменшуватися. Це не очевидно, тому треба використати значення від 0 до 10. Результат розрахунків:

середня абсолютна нев'язка дорівнює 1,8092.

середня квадратична нев'язка дорівнює 5,7062.

Приклад впливу ваги правила №23 на середню квадратичну нев'язку представлене в табл. 2.7.

Таблиця 2.7

Середня квадратична нев’язка від ваги правила №23

Значення коефіцієнта	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**
Середня квадратична нев’язка	5,5134	5,4867	5,4810	5,5198	5,5201
Значення коефіцієнта	**0,6**	**0,7**	**0,8**	**0,9**	**1,0**
Середня квадратична нев’язка	5,5171	5,4699	5,4677	5,4732	5,4706

Отже, оптимальна вага правила №23 дорівнює 0,8 коли нев’язка дорівнює 5,4677. Графік даної залежності наведено на рис. 2.13.

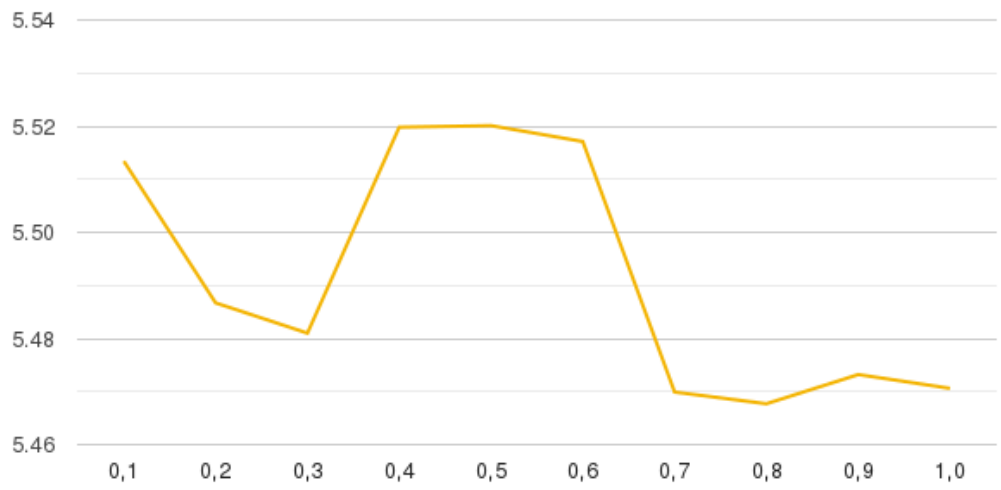


Рис. 2.13. Вплив ваги на нев’язку

Програма розрахунку нев’язки для системи з різними коефіцієнтами правил:

```
n=10;
a=0:1/(n-1):1;
b=0:1/(n-1):1;
c=0:1/(n-1):1;
inp=zeros(n*n,3);
```

```
out=zeros(n*n,1);
l=1;
for i=1:n
     for j=1:n
          for k=1:n
inp(l,1)=a(i);
inp(l,2)=b(j);
inp(l,3)=c(k);
out(l)=a(i)*b(j)*c(k);
l=l+1;
end
     end
          end
ff=readfis('TaskTest2');
new_ff = ff;
numrule = length(ff.rule);
for i=1:numrule
% for i=23:1:23
min_r = 100;
opt_w = 10;
     for w=0.1:0.1:1
new_ff.rule(i).weight=w;
outff=evalfis(inp,new_ff);
residual = sum((outff-out).^2)/(n*n*n);
if residual<min_r
min_r = residual;
opt_w=w;
     end
disp('W = ');
disp(w);
disp('current_weight of this rule = ');
disp(residual);
disp('optimal_weight of this rule = ');
disp(min_r);
```

```
      end
new_ff.rule(i).weight=opt_w;
writefis(new_ff, 'TaskTest2');
           end
```

Вагові коефіцієнти для всіх 23 правил до та після оптимізації представлене в таблиці 2.8.

Таблиця 2.8

Вага правил

Правило	Коеф без оптим.	Коеф з оптим.
1	1	0,1
2	1	0,2
3	1	0,1
4	1	0,2
5	1	0,3
6	1	0,1
7	1	0,6
8	1	0,1
9	1	0,1
10	1	0,3
11	1	0,6
12	1	0,1
13	1	0,1
14	1	0,1
15	1	0,1
16	1	0,1
17	1	0,3
18	1	0,1
19	1	0,2
20	1	0,1
21	1	0,7
22	1	0,7
23	1	0,7

Завдяки оптимізації нев’язка стала дорівнювати 1,6709 замість 5,7062.

Отже, розроблена частина моделі оцінки, а саме, алгоритми оптимізації значень вагових коефіцієнтів правил по критерію мінімальної середньої квадратичної нев’язки, який для конкретного випадку зменшує нев’язку з 5,7062 до 1,6709.

Формування оптимальних параметрів функцій належності. Аналіз літератури за тематикою нечіткої логіки [126, 155 – 159] дозволяє зробити висновок про те, що значення функцій належності впливають на результат нечіткого логічного виведення. Тому однією з часткових задач при розробці моделі оцінки ефективності та стану системи захисту персональних даних є задача підбору таких форм цих функцій, які забезпечують найкращу якість результатів нечіткого виведення, тобто найменшу розбіжність між експериментальними даними та результатами моделювання. При параметричному заданні функцій належності сформульована часткова задача оптимізації, яка формулюється таким чином: знайти такі параметри функцій належності, які забезпечують найкращу якість нечіткого логічного виведення, а саме, мінімальну нев'язку між експериментальними даними та результатами моделювання.

Нехай експериментальні точки згенеровані з залежності виду e^{ab}, тоді код який буде генерувати тисячу точок та обчислювати значення функції має вигляд:

```
n=10;
a=0:1/(n-1):1;
b=0:1/(n-1):1;
c=0:1/(n-1):1;
inp=zeros(n*n,3);
out=zeros(n*n,1);
l=1;
for i=1:n
     for j=1:n
          for k=1:n
inp(l,1)=a(i);
inp(l,2)=b(j);
inp(l,3)=c(k);
out(l)=a(i)*b(j)*c(k);
l=l+1;
```

```
end
     end
          end
```

Код, який буде зчитувати систему нечіткого логічного виведення та обчислювати її значення має вигляд:

```
ff_name = 'Test1';
ff=readfis(ff_name);
new_ff = ff;
a=-2;
b=-2;
c=-2;
min_r = 100;
for x = 1:3
start = -0.5;
end_s = 1.5;
     for i=1:3
          for t=start:0.1:end_s
               for j = start+0.5:0.1:end_s+0.5
                    for k=start+0.5:0.1:end_s+0.5
 if((t < j && t > a) && (j<k && j > b))
%Обчислення максимальної абсолютної нев'язки
     end
          end
               end
                    end
 disp('New par of values into input :');
 disp(x);
 disp('and term :');
 disp(i);
 par = [a,b,c]
 new_ff=setfis(new_ff,'input',x,'mf',i,'params',par);
 start=start+0.1;
 end_s=end_s+0.1;
end
     end
```

В наступному циклі генеруються усі можливі значення термів та записуються оптимальні значення в змінні, які потім вносяться в систему нечіткого виведення. В якості критерію оптимальності використовується середня абсолютна нев'язка. Лістинг програми:

```
par=[t, j, k];
new_ff=setfis(new_ff,'input',x,'mf',i,'params',par);
outff=evalfis(inp,new_ff);
residual = max(abs(outff-out));
if residual<min_r
residual = sum(abs(outff-out))/(n*n*n);
a=t;
b=j;
c=k;
end
```

За умови, що поточна нев'язка є нижчою ніж попередня, то вона встановлюється як оптимальна, передаючи в змінну `min_r`, після чого встановлюються поточні значення терму в змінні *a*, *b* та *c*, після чого по закінченню ітерації циклу вносимо їх, як оптимальні значення в `fis`-файл.

Вхідні терми системи до оптимізації:

```
[Input1]
MF1='L':'trimf',[-0.4 0 0.4]
MF2='M':'trimf',[0.1 0.5 0.9]
MF3='H':'trimf',[0.6 1 1.4]
[Input2]
MF1='L':'trimf',[-0.4 0 0.4]
MF2='M':'trimf',[0.1 0.5 0.9]
MF3='H':'trimf',[0.6 1 1.4]
[Input3]
MF1='L':'trimf',[-0.4 0 0.4]
MF2='M':'trimf',[0.1 0.5 0.9]
MF3='H':'trimf',[0.6 1 1.4]
```

Нев'язка до оптимізації: 5,0371

Вхідні терми після оптимізації:

```
[Input1]
MF1='L':'trimf',[-0.1 0.4 0.5]
MF2='M':'trimf',[0.5 1 2]
MF3='H':'trimf',[0.2 1.8 1.9]
[Input2]
MF1='L':'trimf',[-0.1 0.4 0.9]
MF2='M':'trimf',[0.6 1.7 2.1]
MF3='H':'trimf',[0 1.7 1.8]
[Input3]
MF1='L':'trimf',[-0.1 0.4 0.6]
MF2='M':'trimf',[0.3 1.1 1.8]
MF3='H':'trimf',[0.1 1.4 1.5]
```

Нев'язка після оптимізації: 0.4000

Алгоритм для вихідної змінної аналогічний.

Терми до оптимізації:

```
[Output1]
MF1='mf1':'trimf',[-5 0 5]
MF2='mf2':'trimf',[0 5 10]
MF3='mf3':'trimf',[5 10 15]
```

Терми після оптимізації:

```
[Output1]
MF1='L':'trimf',[-1 0.5 1]
MF2='M':'trimf',[0 4 4.5]
MF3='H':'trimf',[4.5 5 7]
```

Отже, результати рішення задачі – параметри функцій належності, які забезпечують найкращу якість нечіткого логічного висновку, а саме, мінімальну нев'язку між експериментальними даними та результатами моделювання представлені в табл. 2.9.

Таблиця 2.9

Параметри функцій належності

Змінна	Low	Mid	High
Input 1 Before	[-0.4 0 0.4]	[0.1 0.5 0.9]	[0.6 1 1.4]
Input 1 After	[-0.1 0.4 0.5]	[0.5 1 2]	[0.2 1.8 1.9]
Input 2 Before	[-0.4 0 0.4]	[0.1 0.5 0.9]	[0.6 1 1.4]
Input 2 After	[-0.1 0.4 0.9]	[0.6 1.7 2.1]	[0 1.7 1.8]
Input 3 Before	[-0.4 0 0.4]	[0.1 0.5 0.9]	[0.6 1 1.4]
Input 3 After	[-0.1 0.4 0.6]	[0.3 1.1 1.8]	[0.1 1.4 1.5]
Output 1 Before	[-5 0 5]	[0 5 10]	[5 10 15]
Output 2 After	[-1 0.5 1]	[0 4 4.5]	[4.5 5 7]

Структурна схема та схема етапів моделі оцінки стану системи захисту персональних даних представлене на рисунках 2.14 та 2.15.

Рис. 2.14. Структурна схема моделі оцінки стану системи захисту персональних даних

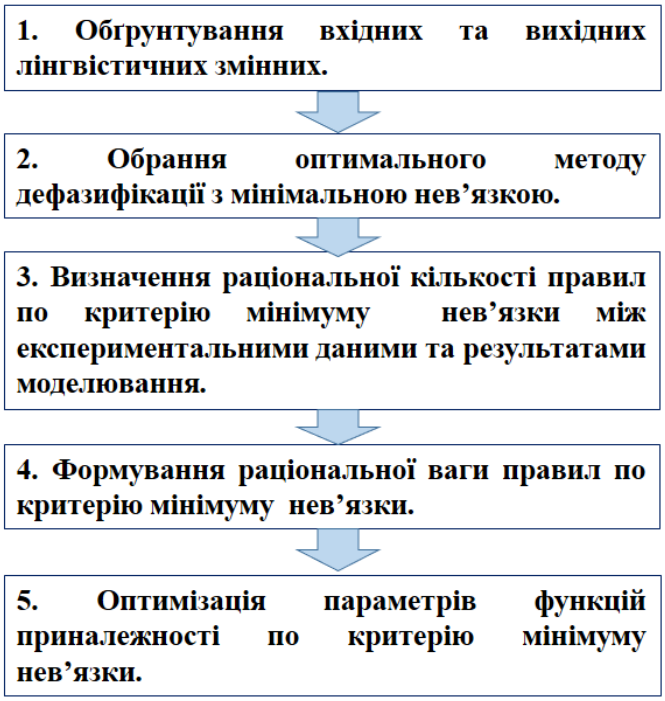


Рис. 2.15. Схема етапів моделі оцінки стану системи захисту персональних даних

Оцінка стану системи захисту персональних даних користувачів системи дистанційного навчання навчального закладу Збройних Сил України виконана на основі запропонованої та описаної в даному розділі моделі (результати в табл. 2.10). Результати експерименту дозволяють отримувати чітку кількісну оцінку ефективності системи та необхідні для прийняття рішення для подальшого удосконалення системи захисту. Отримані дані використані як навчальні дані для нейронні мережі, яка описана в наступному розділі дисертації та використана для прогнозування стану системи захисту персональних даних користувачів системи дистанційного навчання відповідного навчального закладу ЗСУ [57].

Таблиця 2.10

Результати дослідження

Дата дослідження	Ефективність системи	Дата дослідження	Ефективність системи
02.01.2023	0.9955	02.02.2023	0.9999
03.01.2023	0.9999	03.02.2023	0.9997
04.01.2023	0.9999	04.02.2023	0.9998
05.01.2023	0.9997	06.02.2023	0.9999
06.01.2023	0.9998	07.02.2023	0.9932
07.01.2023	0.9999	08.02.2023	0.9925
08.01.2023	0.9999	09.02.2023	0.9911
10.01.2023	0.9999	10.02.2023	0.9998
11.01.2023	0.9997	11.02.2023	0.9999
12.01.2023	0.9965	13.02.2023	0.9999
13.01.2023	0.9951	14.02.2023	0.9999
14.01.2023	0.9999	15.02.2023	0.9997
16.01.2023	0.9999	16.02.2023	0.9998
17.01.2023	0.9999	17.02.2023	0.9999
18.01.2023	0.9998	18.02.2023	0.9999
19.01.2023	0.9999	20.02.2023	0.9965
20.01.2023	0.9999	21.02.2023	0.9954
21.01.2023	0.9995	22.02.2023	0.9922
23.01.2023	0.9955	23.02.2023	0.9998
24.01.2023	0.9921	24.02.2023	0.9999
25.01.2023	0.9999	25.02.2023	0.9999
26.01.2023	0.9999	27.02.2023	0.9998
27.01.2023	0.9999	28.02.2023	0.9998
28.01.2023	0.9997	01.03.2023	0.9999
30.01.2023	0.9996	02.03.2023	0.9999
31.01.2023	0.9999	03.03.2023	0.9999
01.02.2023	0.9999	04.03.2023	0.9997

Висновки до розділу 2

1. Аналіз публікацій за тематикою впровадження штучного інтелекту в методи, способи та процедури кібербезпеки визначає даний напрям як нову тенденцію. Дослідження показало те, що у кібербезпеці використовується кілька різних напрямів штучного інтелекту, а саме, м’які обчислення, нейронні мережі та машинне навчання. Найпоширеніші

методики включають моделі, які використовують штучний інтелект для ідентифікації та моніторингу зловмисних дій, виявлення кіберзагроз і захисту мереж організації. Система штучного інтелекту також може відстежувати поведінку окремої людини або групи, наприклад, виявляти зміни в активності в соціальних мережах або аналізувати моделі трафіку співробітників, щоб визначити тих, хто може готуватися до кіберзлочину.

2. Під час інтеграції штучного інтелекту в кібербезпеку ключовими проблемами для організацій є те, як проектувати та керувати даними, доступними в багатьох системах, і як структурувати дані, щоб зробити їх доступними для когнітивних програм, які можуть включати контроль людини. Разом з цією тенденцією кібербезпека також все більше використовує когнітивні технології. Когнітивні технології на основі штучного інтелекту є невід'ємною частиною цілісного підходу до кібербезпеки, в якому людський фактор керує процесом і відіграє ключову роль. Аналітики вважають, що професіонали з кібербезпеки, які можуть застосувати успішні когнітивні технології матимуть більший успіх у захисті від кібератак.

3. Пом'якшення кіберзагроз за допомогою штучного інтелекту базується на виявлення та ідентифікації зловмисного програмного забезпечення. Штучний інтелект може допомогти ідентифікувати шкідливі файли до того, як вони досягнуть кінцевого користувача, і, отже, може забезпечити значні переваги безпеки. Для виявлення зловмисного програмного забезпечення використовувалося багато різних підходів штучного інтелекту та машинного навчання, зокрема для: 1) пошуку сховищ вихідного коду зловмисного програмного забезпечення за допомогою техніки «SourceFinder»; 2) пошуку певних рядків у файлах, які можуть вказувати на наявність зловмисного програмного забезпечення або зловмисного коду, а також для їх класифікації; 3) виявлення шаблонів у двійкових виконуваних файлах і визначення їх шкідливості; 4) виявлення та

зупинки зловмисного програмного забезпечення на основі використання візуальних двійкових шаблонів, визначених у коді і типу самоорганізованої мережі, яка адаптується з часом до інших завдань.

4. Штучний інтелект можна використовувати для виявлення спаму шляхом аналізу змісту повідомлення та пошуку шаблонів, типових для спаму. Це робиться за допомогою алгоритмів машинного навчання, навчених на великій кількості прикладів спаму та інших повідомлень. У процесі виявлення спаму штучний інтелект часто змінює роль людини та може виявляти, що повідомлення є спамом, не потребуючи втручання людини.

5. Використання штучного інтелекту для систем виявлення вторгнень є новою галуззю, що розвивається. Цей напрям займається розробкою інтелектуальних систем для виявлення, класифікації та реагування на кібератаки. Він призначений для виявлення зловмисної поведінки та припинення її до того, як вона спричинить будь-яку шкоду. Він може бути реалізований, як окрема система або, як додатковий модуль до іншого програмного забезпечення безпеки, наприклад, антивірусних програм. Система виявлення вторгнень зазвичай налаштована за допомогою набору правил, які визначають, що є атакою, наприклад, використання певних слів у темі повідомлення електронної пошти або надсилання занадто великої кількості повідомлень за певний період часу. Система виявлення вторгнень зазвичай налаштована на створення сповіщень про виявлені події, які можуть свідчити про атаку чи спробу вторгнення. Отже, моделі та методи штучного інтелекту можуть виявляти та зупиняти кіберзагрози в реальному часі в системах з обмеженими ресурсами.

6. Природа кібератак, що постійно розвивається, означає, що людям доведеться намагатися не відставати від інформації. Однак за допомогою машинного навчання штучний інтелект може скорочувати дані для швидкого аналізу та забезпечувати відмінне покриття безпеки, не

забираючи багато часу чи енергії на поточні завдання. Варто підкреслити те, що технології ШІ не є високоефективними для всіх форм безпеки. Але підходи на основі штучного інтелекту стають все більш поширеними та економічно ефективними в більшості аспектів кібербезпеки. Дослідження показують, що штучний інтелект позитивно вплинув на кібербезпеку та ризики. Отже, продовження штучного інтелекту та машинного навчання виведе сферу кібербезпеки на новий рівень розвитку.

7. Доцільність концепції підвищення захищеності персональних даних грунтується на наступному:

використання детермінованих і стохастичних алгоритмів прийняття рішення пов’язано з неадекватністю, неповнотою або відсутністю необхідних даних для створення аналітичних виразів. В такому випадку доцільним є апарат математичної логіки, а саме, алгебри логіки – її розділу, який дозволяє формально визначати систему логічних операції над висловлюваннями та в бінарному вигляді дати оцінку істинності цих висловлювань. Для захисту персональних даних саме ці висловлювання є описом стратегії та політики, її способів, методів та процедур або їх складових;

як відомо, будь-яка математична модель має певні обмеження щодо її застосування. Бінарна оцінка висловлювання – це те саме обмеження. Ідея нечітких множин заміняє бінарну оцінку 0 або 1 оцінкою на інтервалі [0, 1];

класичні моделі та методи числення предикатів першого порядку, правила виведення числення висловлювань та продукційних систем виведення є основою так званого нечіткого логічного виведення для отримання адекватної та ефективної моделі прийняття рішення при підвищенні захищеності персональних даних;

адаптивні нечіткі нейронні мережі (гібридні мережі) для прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз. Основна ідея гібридних мереж –

використовувати існуючу вибірку даних для визначення параметрів функцій належності, що найкраще відповідають деякій системі нечіткого виведення. При цьому для знаходження параметрів функцій належності використовуються відомі процедури навчання нейронних мереж.

8. Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України, яка запропонована в роботі, забезпечує ефективне реагування на потік загроз та базується на моделях і методах нечіткої логіки та нейронних мереж. Методика поєднує моделі та методи, які спрямовані на комплексне вирішення наступних завдань: 1) ідентифікація загрози та визначення стану системи захисту персональних даних, а саме, система забезпечує захист в повному обсязі або не забезпечує захист та вимагає застосування способів та засобів, які раніше не були використані; 2) формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або у випадку їх низької ефективності формування стратегії удосконалення та розробки нових; 3) прогнозування стану системи захисту в майбутньому з метою попередження шкідливого впливу загроз. Практична реалізація методики дозволяє забезпечити постійний захист персональних даних користувачів системи дистанційного навчання Збройних Сил України.

9. Модель оцінки стану системи захисту персональних даних, яка пропонується в дисертації, на відміну від існуючих базується на нечіткому логічному виведенні (алгоритм Мамдані). В моделі забезпечено оптимальний метод дефазифікації, раціональна вага та кількість правил, оптимальні параметри функцій належності. Застосування моделі дозволяє отримувати чітку кількісну оцінку ефективності системи, яка необхідна для прийняття рішення для подальшого удосконалення системи захисту.

РОЗДІЛ 3. РОЗРОБКА МЕТОДУ ПРОГНОЗУВАННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ НА ОСНОВІ АДАПТИВНОЇ СИСТЕМИ НЕЙРО-НЕЧІТКОГО ВИВЕДЕННЯ

3.1. Обґрунтування доцільності застосування методу прогнозування на основі нейро-нечіткого логічного виведення

Нечіткі нейронні мережі (або гібридні мережі) поєднують в собі переваги систем нечіткого виведення та нейронних мереж. Перша їх властивість в тому що, вони описують моделі систем у формі правил нечітких продукцій, які, як відомо, характеризуються наочністю та простотою. Друга властивість – для побудови правил нечітких продукцій використовуються методи нейронних мереж, що є більш зручним і менш трудомістким процесом [19, 159].

Нечітка нейронна мережа – це багатошарова НМ, в якій шари виконують функції елементів системи нечіткого виведення. Характерною особливістю цих мереж є можливість використання нечітких правил виведення для розрахунку вихідного сигналу. Нейрони цієї мережі характеризуються набором параметрів, налаштування яких відбувається в процесі навчання, як у звичайних НМ [23 – 25].

Гібридна мережа являє собою багатошарову нейронну мережу спеціальної структури без зворотних зв’язків, у якій використовуються звичайні (не нечіткі) сигнали, ваги і функції активації, а виконання операції підсумовування засновано на використанні фіксованої Т-норми, Т-конорми

чи деякої іншої неперервної операції. При цьому значення входів, виходів і ваг гібридної нейронної мережі являють собою дійсні числа з відрізка [0, 1].

Основна концепція, яка покладена в основу принципу дії моделі гібридних мереж, полягає в тому, щоб використовувати існуючу вибірку даних для визначення параметрів функцій належності, що найкраще відповідають деякій системі нечіткого виведення. При цьому для знаходження параметрів функцій належності використовуються відомі процедури навчання нейронних мереж. Одним з найпоширеніших алгоритмів навчання є алгоритм зворотного поширення помилки (backpropagation). Цей алгоритм являє собою ітеративний градієнтний алгоритм мінімізації середньоквадратичного відхилення значень виходу від бажаних значень (мінімізації помилки) у багатошарових нейронних мережах [32, 34, 47].

У пакеті Fuzzy Logic Toolbox системи MATLAB гібридні мережі реалізовані у формі так званої адаптивної системи нейро-нечіткого виведення – Adaptive Neuro Fuzzy Inference System (ANFIS). З одного боку, гібридна мережа ANFIS являє собою нейронну мережу з єдиним виходом і декількома входами, що являють собою нечіткі лінгвістичні змінні. При цьому терми вхідних лінгвістичних змінних описуються стандартними для системи MATLAB функціями належності, а терми вихідної змінної представляються лінійною чи постійною функцією належності [23, 48].

З іншого боку, гібридна мережа ANFIS являє собою систему нечіткого виведення типу алгоритму Сугено нульового чи першого порядку, у якій кожне з правил нечітких продукцій має постійну вагу, рівну 1. У системі MATLAB користувач має можливість редагувати і налаштовувати гібридні мережі ANFIS аналогічно системам нечіткого виведення, використовуючи всі можливості та засоби пакета Fuzzy Logic Toolbox [23, 83].

У пакеті Fuzzy Logic Toolbox системи MATLAB редактор ANFIS дозволяє створювати (або завантажувати) конкретну модель адаптивної

системи нейро-нечіткого виведення, виконувати її навчання, візуалізувати її структуру, змінювати і налагоджувати її параметри, а також використовувати налагоджену мережу для одержання результатів нечіткого виведення [23].

3.2. Розробка методу прогнозування стану системи захисту персональних даних на основі адаптивної системи нейро-нечіткого виведення

В якості ефективного та добре апробованого наукового методу прогнозування стану системи захисту персональних даних в дисертації обрано адаптивну мережеву нечітку систему виведення ANFIS, яка була запропонована Джи-Шинг Роджером Джангом (Jyh-Shing Roger Jang) в 1993 році [159]. Модель нечіткого логічного виведення, навчається класичними градієнтними алгоритмами, є універсальним апроксиматором та є п’ятишаровою штучною нейронною мережею прямого поширення сигналу. Схема методу представлена на рис. 3.1.

Етапи методу прогнозування. Формування навчальних даних (Training Data) [57]. В якості навчальних даних для моделі прогнозу використані дані експерименту оцінки стану системи захисту персональних даних (табл. 2.10). Дані з 28.02.2023 по 04.03.2023 використані для перевірки точності розробленої моделі прогнозу. В табл. 3.1 та 3.2 сформовані навчальні данні для створення моделі гібридної мережі та перевірочні дані відповідно.

Створено файл data_shapran_2.dat: 4 вхідні та 1 вихідна змінна (рис. 3.2).

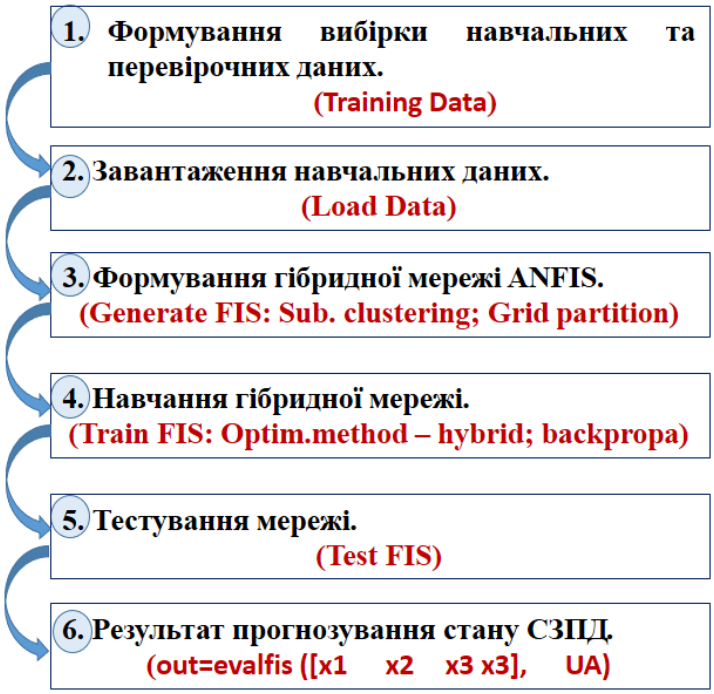
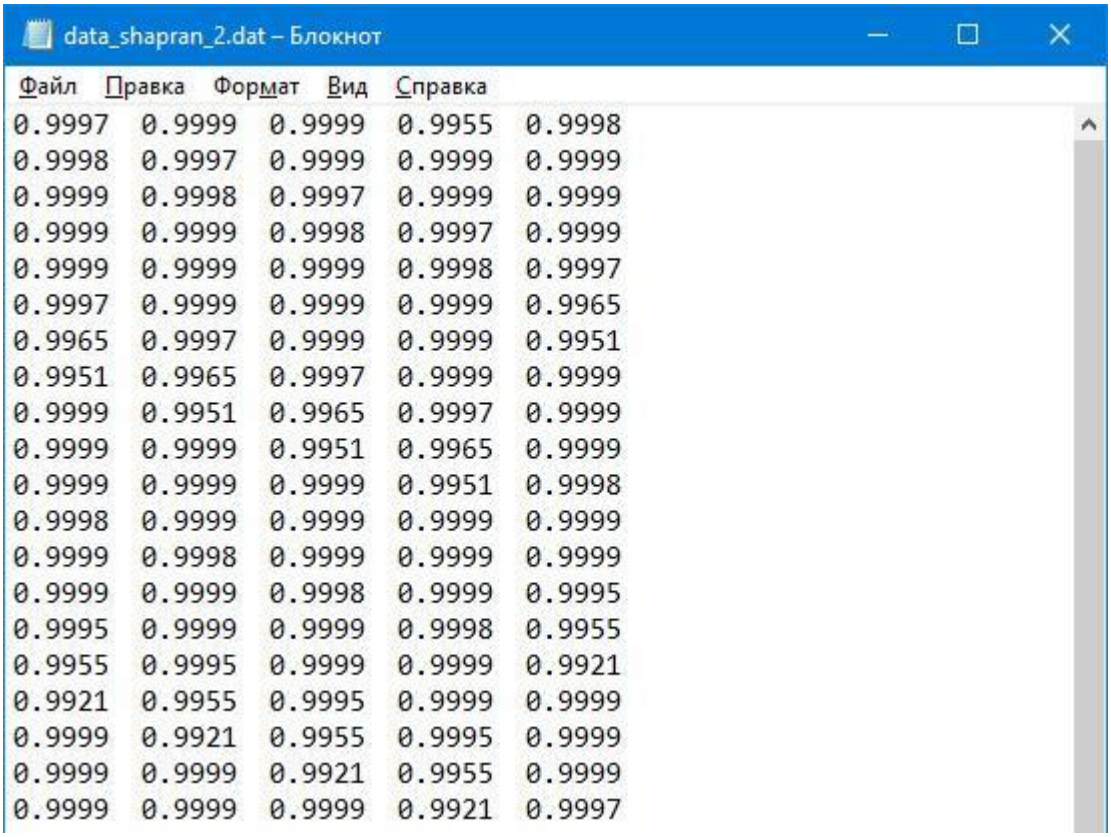


Рис. 3.1. Схема етапів методу прогнозування стану системи захисту персональних даних



data_shapran_2.dat – Блокнот

Файл Правка Формат Вид Справка

0.9997	0.9999	0.9999	0.9955	0.9998
0.9998	0.9997	0.9999	0.9999	0.9999
0.9999	0.9998	0.9997	0.9999	0.9999
0.9999	0.9999	0.9998	0.9997	0.9999
0.9999	0.9999	0.9999	0.9998	0.9997
0.9997	0.9999	0.9999	0.9999	0.9965
0.9965	0.9997	0.9999	0.9999	0.9951
0.9951	0.9965	0.9997	0.9999	0.9999
0.9999	0.9951	0.9965	0.9997	0.9999
0.9999	0.9999	0.9951	0.9965	0.9999
0.9999	0.9999	0.9999	0.9951	0.9998
0.9998	0.9999	0.9999	0.9999	0.9999
0.9999	0.9998	0.9999	0.9999	0.9999
0.9999	0.9999	0.9998	0.9999	0.9995
0.9995	0.9999	0.9999	0.9998	0.9955
0.9955	0.9995	0.9999	0.9999	0.9921
0.9921	0.9955	0.9995	0.9999	0.9999
0.9999	0.9921	0.9955	0.9995	0.9999
0.9999	0.9999	0.9921	0.9955	0.9999
0.9999	0.9999	0.9999	0.9921	0.9997

Рис. 3.2. Навчальні дані

Таблиця 3.1

Навчальні дані для створення моделі гібридної мережі

Вхідні змінні				**Вихідна змінна**
перша	**друга**	**третя**	**четверта**	
0.9997	0.9999	0.9999	0.9955	0.9998
0.9998	0.9997	0.9999	0.9999	0.9999
0.9999	0.9998	0.9997	0.9999	0.9999
0.9999	0.9999	0.9998	0.9997	0.9999
0.9999	0.9999	0.9999	0.9998	0.9997
0.9997	0.9999	0.9999	0.9999	0.9965
0.9965	0.9997	0.9999	0.9999	0.9951
0.9951	0.9965	0.9997	0.9999	0.9999
0.9999	0.9951	0.9965	0.9997	0.9999
0.9999	0.9999	0.9951	0.9965	0.9999
0.9999	0.9999	0.9999	0.9951	0.9998
0.9998	0.9999	0.9999	0.9999	0.9999
0.9999	0.9998	0.9999	0.9999	0.9999
0.9999	0.9999	0.9998	0.9999	0.9995
0.9995	0.9999	0.9999	0.9998	0.9955
0.9955	0.9995	0.9999	0.9999	0.9921
0.9921	0.9955	0.9995	0.9999	0.9999
0.9999	0.9921	0.9955	0.9995	0.9999
0.9999	0.9999	0.9921	0.9955	0.9999
0.9999	0.9999	0.9999	0.9921	0.9997
0.9997	0.9999	0.9999	0.9999	0.9996
0.9996	0.9997	0.9999	0.9999	0.9999
0.9999	0.9996	0.9997	0.9999	0.9999
0.9999	0.9999	0.9996	0.9997	0.9999
0.9999	0.9999	0.9999	0.9996	0.9997
0.9997	0.9999	0.9999	0.9999	0.9998
0.9998	0.9997	0.9999	0.9999	0.9999
0.9999	0.9998	0.9997	0.9999	0.9932
0.9932	0.9999	0.9998	0.9997	0.9925
0.9925	0.9932	0.9999	0.9998	0.9911
0.9911	0.9925	0.9932	0.9999	0.9998
0.9998	0.9911	0.9925	0.9932	0.9999
0.9999	0.9998	0.9911	0.9925	0.9999
0.9999	0.9999	0.9998	0.9911	0.9999
0.9999	0.9999	0.9999	0.9998	0.9997
0.9997	0.9999	0.9999	0.9999	0.9998
0.9998	0.9997	0.9999	0.9999	0.9999
0.9999	0.9998	0.9997	0.9999	0.9999
0.9999	0.9999	0.9998	0.9997	0.9965
0.9965	0.9999	0.9999	0.9998	0.9954

Таблиця 3.2

Перевірочні дані моделі гібридної мережі

Вхідні змінні				Вихідна змінна
перша	**друга**	**третя**	**четверта**	
0.9998	0.9999	0.9999	0.9998	0.9998
0.9998	0.9998	0.9999	0.9999	0.9999
0.9999	0.9998	0.9998	0.9999	0.9999
0.9999	0.9999	0.9998	0.9998	0.9999
0.9999	0.9999	0.9999	0.9998	0.9997

1) Завантаження навчальних даних. Інтерфейс зображено на рис.3.3.

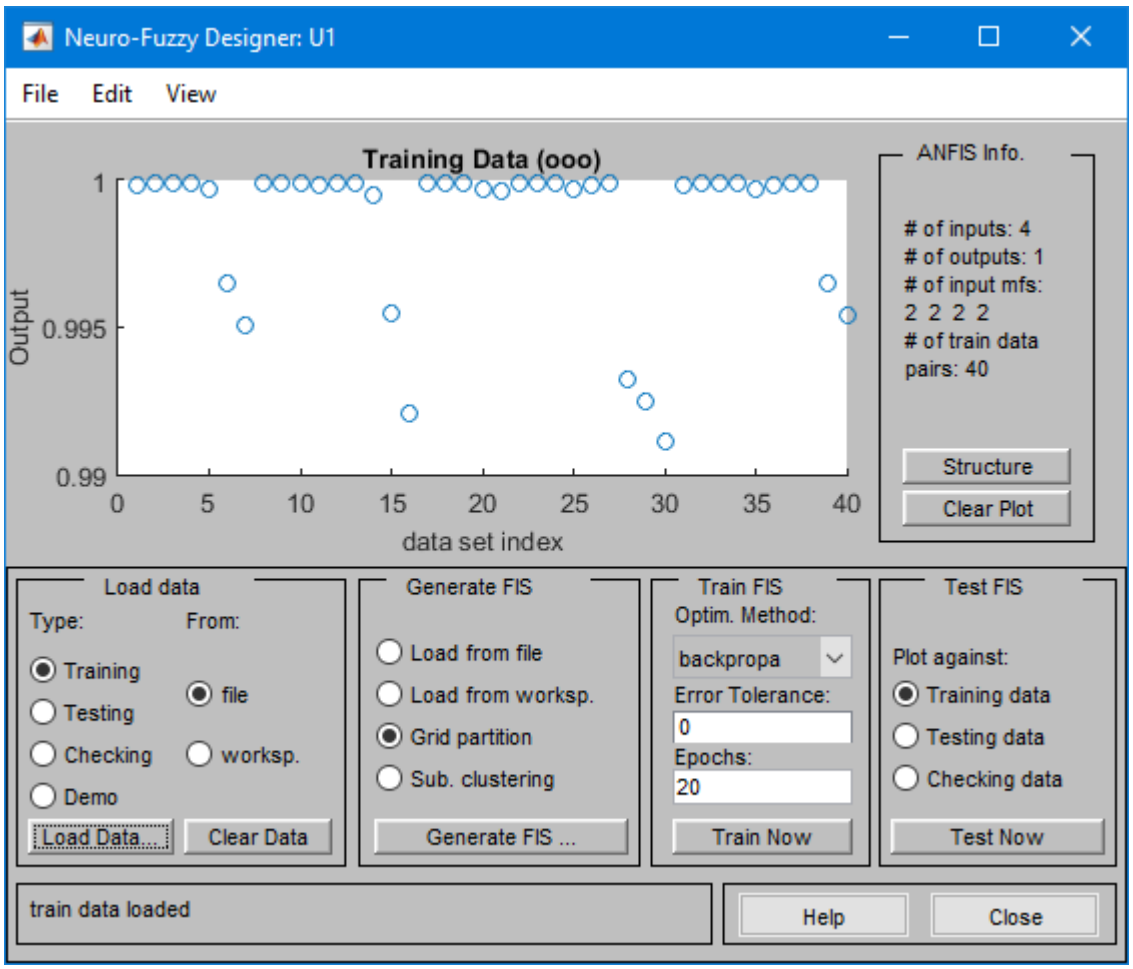


Рис. 3.3. Навчальні дані (інтерфейс ANFIS)

2) Налаштування нечіткої кластеризації. Інтерфейс вхідних даних на рис. 3.4.

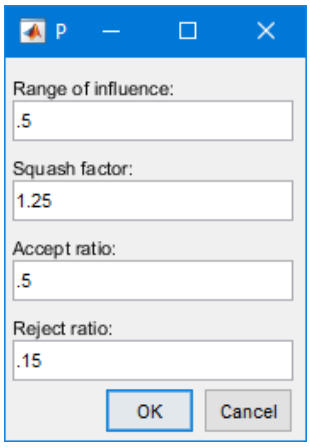


Рис. 3.4. Інтерфейс кластеризації

3) Формування гібридної мережі (рис.3.5, 3.6).

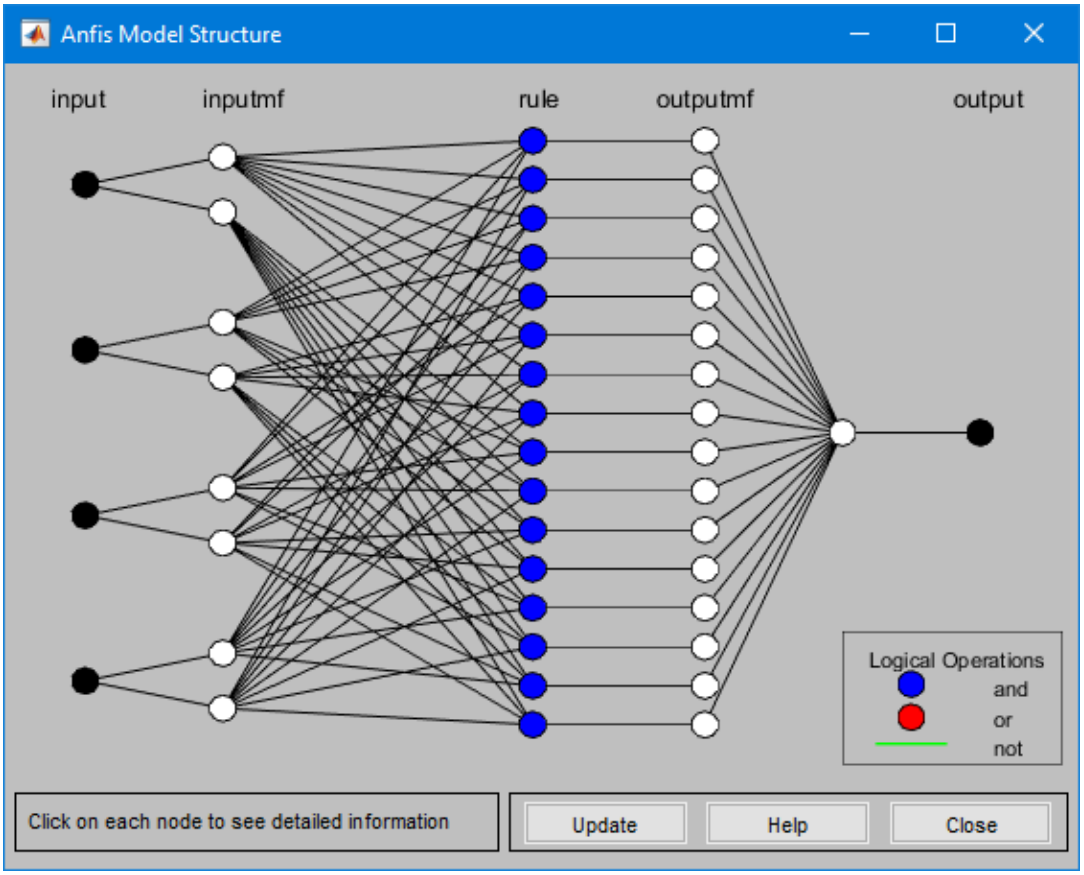


Рис. 3.5. Гібридна мережа

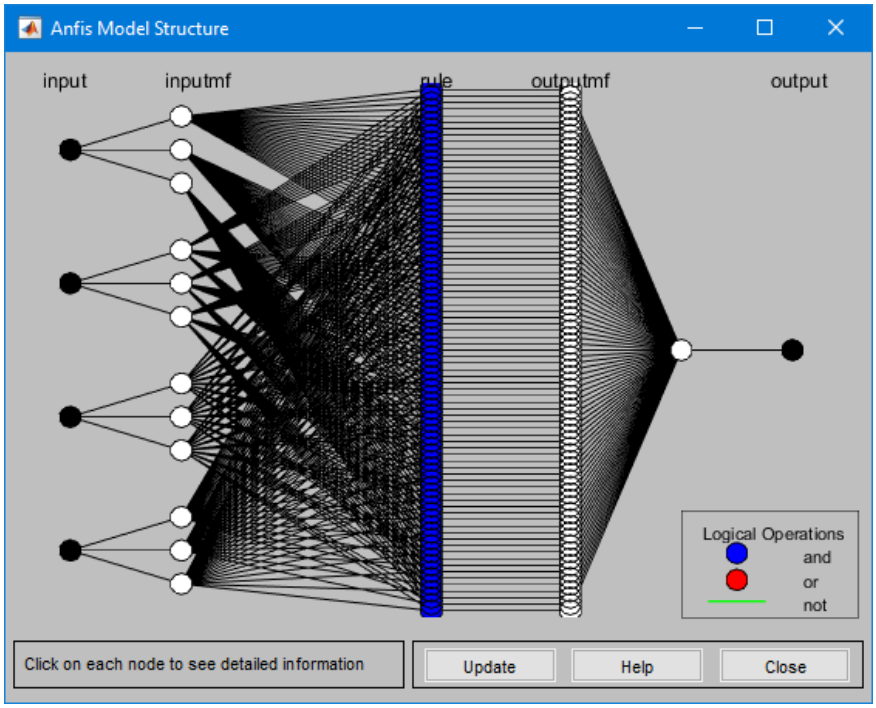


Рис. 3.6. Гібридна мережа

4) Навчання мережі гібридним методом (рис. 3.7)

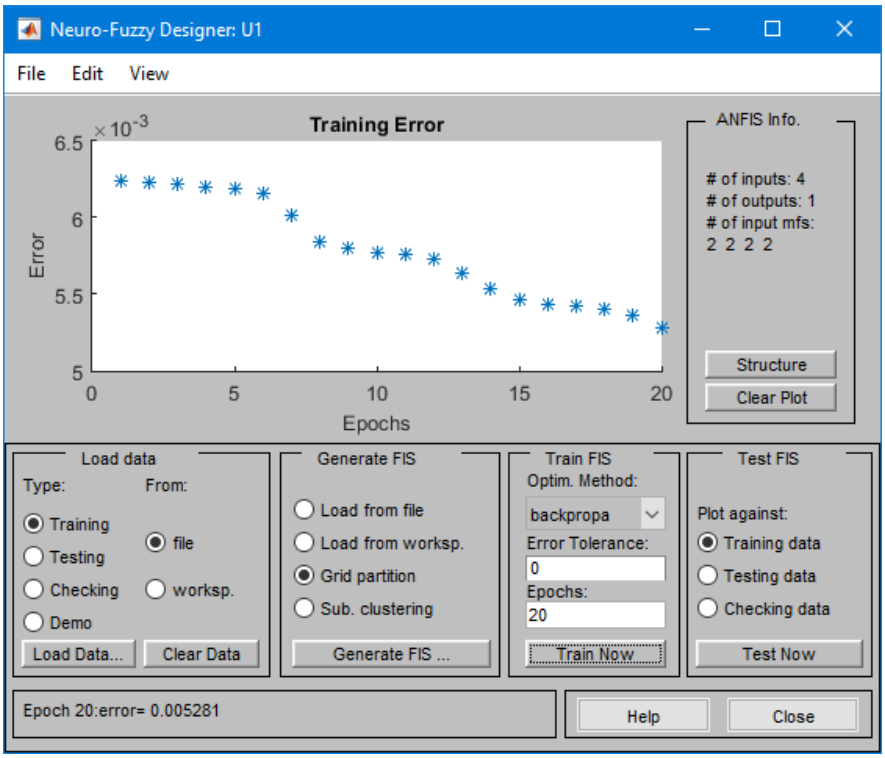


Рис. 3.7. Навчання мережі

На рис. 3.8 надана модель FIS для гібридної мережі, яка сформована для модельного прикладу, та на рис. 3.9 відповідні правила виведення.

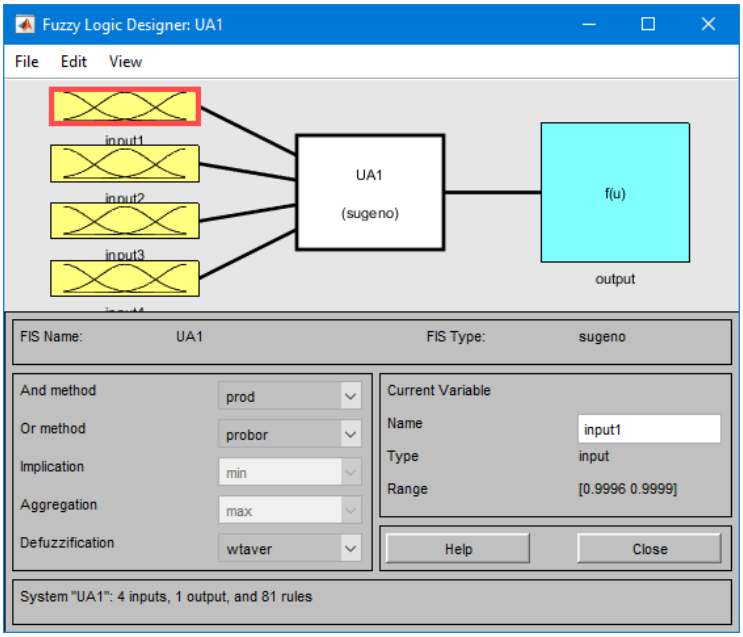


Рис. 3.8. Модель нечіткого виведення за алгоритмом Сугено

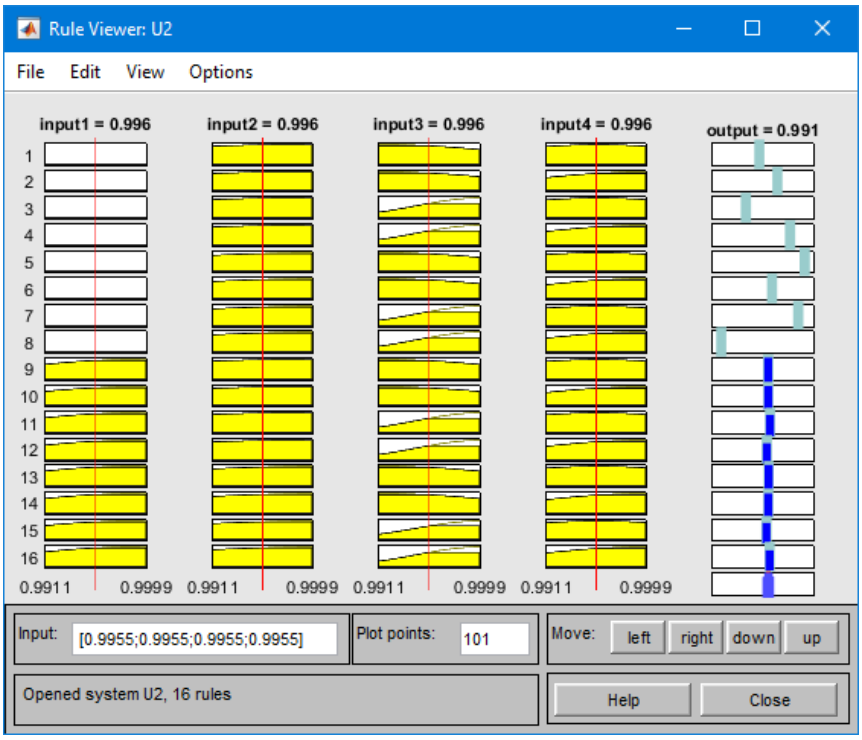


Рис. 3.9. Правила виведення

Приклад функції належності надано на рис. 3.10.

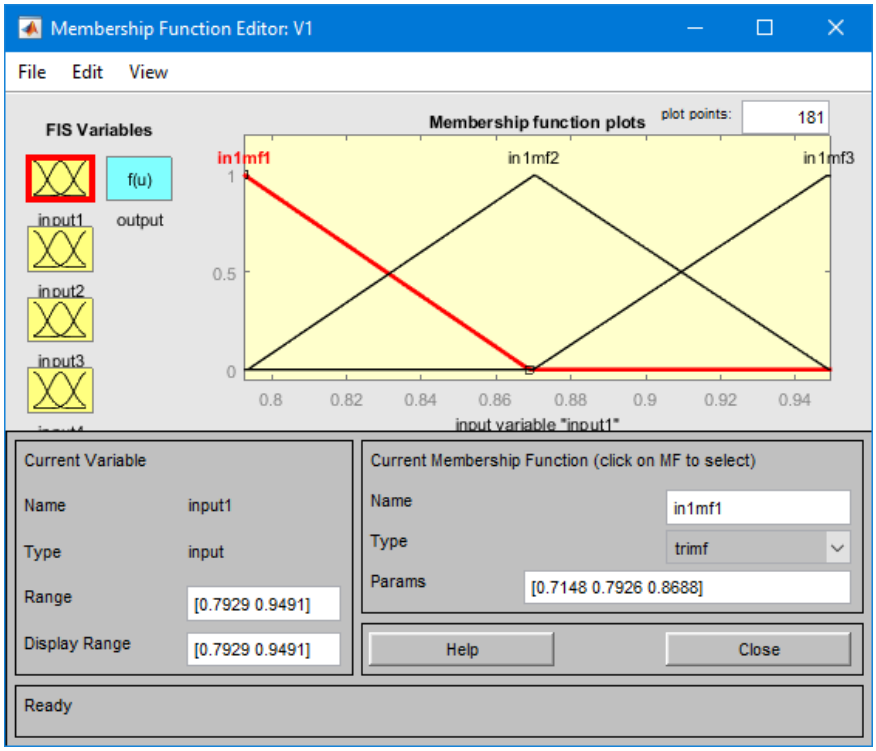


Рис. 3.10. Функція належності

Результати моделювання прогнозу ефективності системи свідчать про збіг даних з реальними значеннями, які були обрані для перевірки адекватності та точності методу (таблиця 3.3).

Результат функції evalfis:

```
>> out = evalfis([  0.9998    0.9999    0.9999    0.9998;
                    0.9998    0.9998    0.9999    0.9999;
                    0.9999    0.9998    0.9998    0.9999;
                    0.9999    0.9999    0.9998    0.9998;
                    0.9999    0.9999    0.9999    0.9998;],U1)
out =
            0.9997
            0.9998
            0.9999
            0.9999
            0.9996
```

Таблиця 3.3

Оцінка точності прогнозу

Експеримент	Прогноз	Похибка, %
0.9998	0.9997	0,01
0.9999	0.9998	0,01
0.9999	0.9999	0
0.9999	0.9999	0
0.9997	0.9996	0,01

Отже, середня похибка прогнозу δ=0,006 %.

Спрощена схема моделювання надана на рисунку 3.11.

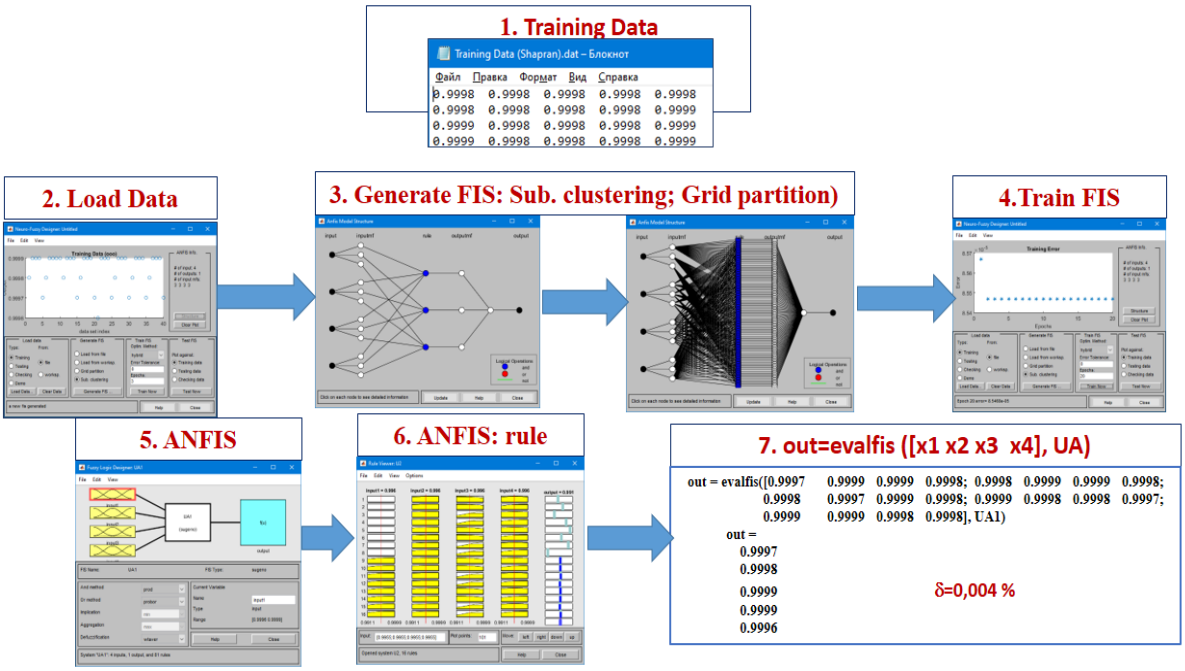


Рис. 3.11. Спрощена схема моделювання

Отже, дослідження розробленого методу прогнозування стану системи захисту персональних даних на основі нечіткої моделі гібридної мережі дозволяє зробити висновок про достатню ступінь його відповідності реальним вихідним даним та рекомендувати цей метод до практичного використання. Також варто зазначити те, що нечіткі моделі адаптивних

систем нейронечіткого висновку можуть вважатися конструктивним інструментом для розробок в кібербезпеці [44, 57].

Висновки до розділу 3

1. Дослідження моделей та методів прогнозу стану складних процесів та систем вимагає звернути увагу на нечіткі нейронні мережі або гібридні мережі, які поєднують в собі переваги систем нечіткого виведення та нейронних мереж. Вони описують моделі систем у формі правил нечітких продукцій, які характеризуються наочністю та простотою. Але для побудови правил нечітких продукцій доцільно застосовувати методи нейронних мереж, що є більш зручним і менш трудомістким процесом. Нечітка нейронна мережа – це багатошарова НМ, в якій шари виконують функції елементів системи нечіткого виведення. Характерною особливістю цих мереж є можливість використання нечітких правил виведення для розрахунку вихідного сигналу. Нейрони цієї мережі характеризуються набором параметрів, налаштування яких відбувається в процесі навчання, як у класичних нейронних мереж.

2. Основна ідея, яка покладена в основу принципу дії моделі гібридних мереж, полягає в тому, щоб використовувати існуючу вибірку даних для визначення параметрів функцій належності, що найкраще відповідають деякій системі нечіткого виведення. При цьому для знаходження параметрів функцій належності використовуються відомі процедури навчання нейронних мереж.

3. Розроблений в дисертації метод прогнозування стану системи захисту персональних даних користувачів системи дистанційного навчання базується на технології адаптивної нейронної нечіткої мережевої системи

виведення ANFIS (Adaptive Neuro-Fuzzy Inference System). Використання методу дозволяє прогнозувати ефективність системи захисту та планувати заходи щодо забезпечення підвищення захищеності персональних даних.

4. Дослідження розробленого методу прогнозування стану системи захисту персональних даних на основі нечіткої моделі гібридної мережі дозволяє зробити висновок про високу ступінь його адекватності реальним вихідними даними та рекомендувати цей метод до практичного використання. За результатами перевірки середня похибка методу складає 0,006 %.

5. Також варто зазначити те, що нечіткі моделі адаптивних систем нейронечіткого виведення можуть вважатися ефективним інструментом для інших розробок в кібербезпеці.

РОЗДІЛ 4. РЕКОМЕНДАЦІЇ ЩОДО ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ НАУКОВИХ РЕЗУЛЬТАТІВ

4.1. Рекомендації щодо реалізації розроблених наукових результатів

Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України забезпечує ефективне реагування на потік загроз та базується на формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або у випадку їх низької ефективності формування стратегії удосконалення та розробки нових, тому рекомендуються наступні.

Програмні засоби захисту. Програмні засоби захисту – це програми і служби, які захищають операційні системи, бази даних та інші служби, що працюють на робочих станціях користувачів СДН, портативних пристроях і серверах. Існує кілька програмних технологій, які використовуються для захисту СДН.

Апаратні засоби захисту. Апаратні засоби захисту мають у складі: пристрої брандмауера, системи виявлення вторгнень (IDS), системи захисту від вторгнення (IPS) та системи фільтрації вмісту.

Мережеві технології захисту. Віртуальна приватна мережа (VPN) – це безпечна віртуальна мережа, що використовує загальнодоступну мережу (Інтернет). Безпека VPN полягає у шифруванні вмісту пакета при передачі між кінцевими точками [82].

Контроль доступу до мережі (NAC) вимагає виконання набору перевірок, перш ніж дозволити пристрою підключатися до мережі. Деякі з

видів перевірки – це оновлення антивірусного програмного забезпечення або операційної системи.

Безпеку безпроводової точки доступу доцільно забезпечити за допомогою аутентифікації і шифрування.

Хмарні технології захисту. Технологічні контрзаходи в сучасних умовах включають також хмарні технології. Хмарні технології реалізують технологічний компонент захисту СДН на базі провайдера хмарних обчислень. Програмне забезпечення як послуга (SaaS) дозволяє користувачам отримувати доступ до прикладного програмного забезпечення та баз даних. Хмарні провайдери управляють інфраструктурою. Користувачі зберігають дані на серверах хмарного провайдера. Інфраструктура як послуга (IaaS) забезпечує віртуальні обчислювальні ресурси через Інтернет. Провайдер використовує апаратне забезпечення, програмне забезпечення, сервери і компоненти зберігання. Віртуальні пристрої безпеки – це внутрішнє віртуальне середовище з попередньо запакованою і захищеною операційною системою, яка працює на віртуалізованому обладнанні [87].

Програма інформування про безпеку надзвичайно важлива для закладу СДН. Співробітник може не навмисно вчиняти потенційно небезпечні дії, через те, що просто не знає, як вчинити безпечно.

Існує кілька способів реалізації формальної навчальної програми: зробити тренінг з безпеки необхідним елементом для початку роботі у закладі СДН; зробити процедури необхідні для безпечного використання частиною службових зобов’язань співробітника; проведення очних тренінгів; проведення онлайн-курсів. Таке навчання має запроваджуватися на регулярних засадах, оскільки нові загрози з’являються постійно [98].

Застосування всіх правил політики безпеки, а саме, правил для навчального закладу, які включають правила поведінки для користувачів і адміністраторів і визначають системні вимоги. Такі цілі, правила і вимоги в

сукупності забезпечують безпеку мережі, даних і комп'ютерних систем всередині організації.

Застосування стандартів, які допомагають IT-персоналу підтримувати узгодженість в роботі мережі. Стандартні документи надають технології, які необхідні конкретним користувачам або програмам для виконання робочих вимог або задають критерії, яких повинна дотримуватися організація при виборі таких технологій.

Застосування методичних рекомендацій – пропозицій щодо того, як робити речі більш ефективно і безпечно. Вони схожі на стандарти, але більш гнучкі і зазвичай не є обов'язковими. Ці рекомендації визначають, як розробляються стандарти і гарантують дотримання загальних політик безпеки.

Варто звернути увагу на процедурні документи, які більш докладні і детальні, ніж стандарти і рекомендації і містять у собі деталі реалізації, зазвичай з покроковими інструкціями. Фахівцям з галузі безпеки необхідно забезпечити захист інформації всередині організації. Це монументальне завдання і необґрунтовано очікувати, що одна людина матиме всі необхідні для цього знання.

Застосування комплексної структури для управління інформаційною безпекою. Міжнародна організація зі стандартизації (ISO)/Міжнародна електротехнічна комісія (IEC) розробила комплексну структуру для управління інформаційною безпекою. Модель кібербезпеки ISO для фахівців з кібербезпеки відіграє таку ж роль, що і мережна модель OSI для інженерів мереж. Обидві моделі забезпечують основу для розуміння і виконання складних завдань спрямованих на забезпечення безпеки.

ISO/IEC 27000 – це стандарт інформаційної безпеки, опублікований у 2005 році і переглянутий в 2013 році. ISO публікує стандарти ISO 27000. Незважаючи на те, що стандарти не обов'язкові, більшість країн використовують їх як основу для забезпечення інформаційної безпеки.

ISO 27000 – це універсальна структура для кожного типу організації. Для ефективного використання структури, організація повинна визначити які галузі, цілі управління та засоби контролю будуть застосовуватися у її діяльності та середовищі.

Цілі контролю ISO 27001 служать контрольним переліком. Перший крок, до якого вдається організація, – це визначення того, чи можуть бути застосовані ці контрольні цілі до неї. Різні групи в межах організації можуть відповідати за дані в кожному з можливих станів. Наприклад, група безпеки мережі відповідає за дані під час передачі. Програмісти і користувачі відповідають за дані під час обробки. Фахівці з апаратної і серверної підтримки відповідають за збережені дані.

Елементи управління ISO спеціально визначають цілі безпеки для даних в кожному з трьох станів. Цілі управління ISO 27001 безпосередньо пов’язані з політикою, процедурами і керівними принципами кібербезпеки організації, які визначає вище керівництво. Елементи управління ISO 27002 забезпечують технічний напрям. Наприклад, вище керівництво встановлює політику, яка визначає захист всіх даних, що надходять до організації або виходять з неї. Реалізація технології для досягнення цілей політики не передбачає управління згори. Відповідальність IT-фахівців полягає у належному впровадженні та налаштуванні обладнання, яке використовується для виконання директив, встановлених керівництвом [100 – 108].

Наступні рекомендації охоплюють:

1) Контроль фізичного доступу – фізичні бар’єри, які використовуються для запобігання прямого контакту з системами. Мета полягає в тому, щоб запобігти несанкціонованому фізичному доступу користувачів до об’єктів, устаткування та інших ресурсів організації. Контроль фізичного доступу визначає, хто може увійти (або вийти), де вони можуть увійти (або вийти), і коли вони можуть увійти (або вийти).

2) Логічні засоби контролю доступу – апаратні і програмні рішення, які використовуються для управління доступом до ресурсів і систем. Ці технологічні рішення включають інструменти та протоколи, які використовуються комп'ютерними системами для ідентифікації, аутентифікації, авторизації та звітності.

3) Адміністративні засоби контролю доступу – політики і процедури, визначені організаціями для реалізації і забезпечення дотримання всіх аспектів контролю за несанкціонованим доступом. Адміністративний контроль зосереджений на персоналі і ділових практиках.

Контроль цілісності даних на основі використання хешування – це інструмент, який забезпечує цілісність даних, беручи двійкові дані (повідомлення) і створюючи з них вихідне значення фіксованої довжини, що називається хеш-значенням або дайджестом повідомлення. Хешування – це одностороння математична функція, яку відносно легко обчислити, але значно складніше повернутися до початкових даних.

Варто нагадати про те що криптографічна хеш-функція має такі властивості:

вхідні дані можуть бути будь-якої довжини;

вихідні дані мають фіксовану довжину;

хеш-функція одностороння і не оборотна;

два різних вхідних значення майже ніколи не приводять до однакових значень хешу.

Серед багатьох сучасних алгоритмів хешування, доцільно використовувати MD5 і SHA. Message Digest 5 (MD5) алгоритм – алгоритм хешування, розроблений Роном Рівестом який генерує 128-бітне хеш-значення. Secure Hash Algorithm (SHA) – був розроблений Національним інститутом стандартів і технологій США (NIST) та може бути використаний у наступних варіантах: SHA-224 (224 біт); SHA-256 (256 біт); SHA-384 (384 біт); SHA-512 (512 біт).

HMAC підсилює алгоритми хешування, використовуючи додатковий секретний ключ в якості вхідних даних для хеш-функції. Використання HMAC йде далі, ніж просто перевірка цілісності шляхом додавання аутентифікації. HMAC використовує спеціальний алгоритм, який об’єднує криптографічну хеш-функцію з секретним ключем.

Використання цифрового підпису. Цифрові підписи для електронних документів забезпечують таку ж функціональність, що і рукописні підписи. За цифровим підписом можна визначити, чи редагувався документ користувачем після підписання. Цифровий підпис – це математичний метод, який використовується для перевірки автентичності та цілісності повідомлення, цифрового документа або програмного забезпечення багатьох країнах цифрові підписи мають таку ж юридичну силу, як документ, підписаний вручну. Цифрові підписи також підтверджують неможливість відмови від авторства документу.

Використання цифрового сертифікату – еквівалент електронного паспорту. Цифровий сертифікат дозволяє користувачам, вузлам і організаціям безпечно обмінюватися інформацією через Інтернет. Зокрема, цифровий сертифікат автентифікує і перевіряє, що користувачі, які надсилають повідомлення, є тими, ким вони себе називають. Цифрові сертифікати також можуть забезпечити конфіденційність для одержувача за допомогою засобів шифрування відповіді.

Забезпечення цілісності даних:

Цілісність об’єктів – всі рядки повинні мати унікальний ідентифікатор, що називають первинним ключем. Цілісність доменів – всі дані, що зберігаються в стовпці, повинні відповідати одному і тому ж формату і єдиному спільному визначенню. Цілісність посилань – зв’язки між таблицями повинні залишатися незмінними. Тому користувач не може видалити запис, пов’язаний з іншими записами.

Визначена користувачем цілісність – набір правил, визначених користувачем, які не відносяться до однієї з інших категорій. Наприклад, клієнт розміщує нові замовлення. Спочатку перевіряється, чи це новий користувач. Якщо це так, додаємо нового клієнта до таблиці клієнтів.

Рекомендації щодо поліпшення доступності. Для забезпечення захисту ВВНЗ повинен знати, які апаратні і програмні активи у нього є. Управління активами включає в себе повну інвентаризацію апаратного та програмного забезпечення. Це означає, що навчальний заклад повинен знати всі компоненти, які можуть піддаватися ризикам безпеки, зокрема: апаратні системи; кожна операційна система; кожний апаратний мережний пристрій; усі мережеві операційні системи; кожний програмний застосунок та бібліотека. Доцільно вибрати автоматичне рішення для відстеження активів.

Класифікація та стандартизація активів – розподіляє усі ресурси ВВНЗ по групах, заснованих на спільних характеристиках. Організація повинна застосовувати систему класифікації активів до документів, записів даних, файлів та дисків; у рамках системи управління ІТ-активами ВВНЗ визначає прийнятні ІТ-активи, які відповідають її цілям.

Ідентифікація загроз – комп’ютерна команда екстреної готовності США (US-CERT) та Міністерство внутрішньої безпеки США підтримують словник загальної уразливості і впливу (CVE). CVE містить стандартний ідентифікаційний номер з коротким описом, посилання на відповідні звіти про уразливості та рекомендації [123-125].

Аналіз ризиків – це процес аналізу небезпек, пов’язаних з природними та антропогенними подіями, для активів організації. Користувач виконує ідентифікацію активів, щоб визначити, які активи захищати.

Пом’якшення наслідків – передбачає зменшення тяжкості втрати чи ймовірності втрати. Для зниження ризиків використовується багато

технічних засобів управління, таких як системи аутентифікації, дозволи на доступ до файлів і брандмауери.

Глибокий захист не забезпечить непроникного кібер-щита, але допоможе організації мінімізувати ризик, утримуючи її на крок попереду кіберзлочинців. Щоб переконатися, що дані та інформація залишаються доступними, ВВНЗ повинен створити різні рівні захисту.

Багатошаровий підхід забезпечує найповніший захист. Якщо кіберзлочинці проникають через один шар, вони все ще повинні подолати ще декілька інших шарів, кожен з яких складніший, ніж попередній. Шарування створює бар'єр множинних захистів, які координують разом, щоб запобігти атакам.

Обмеження доступу до даних та інформації зменшує можливість загрози. ВВНЗ повинен обмежувати доступ, щоб користувачі мали лише рівень доступу, необхідний для виконання своєї роботи.

Різноманітність стосується зміни елементів контролю і процедур на різних рівнях. Порушення одного рівня безпеки не ставить під загрозу всю систему. ВВНЗ може використовувати різні алгоритми шифрування або системи автентифікації для захисту даних у різних станах.

Маскування інформації також може захистити дані та інформацію. ВВНЗ не повинен розкривати інформацію, яку кіберзлочинці можуть використовувати, щоб з'ясувати версію операційної системи, що працює на сервері, або тип використовуваного ним обладнання.

Варто нагадати про те, що складність не обов'язково гарантує безпеку. Занадто велика складність процесу або технології може спричинити неправильні налаштування або недотримання вимог. Простота може насправді покращити доступність.

Забезпечення надлишковості залишається актуальною рекомендацією кібербезпеки та захисту персональних даних користувачів СДН ВВНЗ. Це обумовлено необхідністю виявлення та виправлення так званої єдиної точки

відмови. Одиничною точкою відмови може бути конкретна частина апаратного забезпечення, процес, конкретний фрагмент даних або навіть найважливіша утиліта. Точки відмови – це слабкі ланки ланцюга, які можуть спричинити збій у роботі центру ДН.

Для вирішення проблеми єдиної точки відмови потрібно змінити критичну операцію так, щоб вона не покладалася лише на один елемент. При виконанні критичних операцій ВВНЗ може вбудовувати резервні компоненти, які б могли взяти на себе процес, якщо одна з цих точок відмовить.

Резервування за принципом N + 1 забезпечує доступність системи у разі відмови компонента. Компоненти (*N*) повинні мати щонайменше один резервний компонент (+1).

Надлишковий масив незалежних дисків (RAID) поєднує в собі декілька фізичних жорстких дисків в єдиний логічний блок, що забезпечує надлишковість даних і покращує продуктивність.

RAID приймає дані, які зазвичай зберігаються на одному диску, і розподіляє їх між декількома дисками. При втраті одного з дисків, користувач зможе відновити дані з інших дисків, які також містять ці дані. RAID також може збільшити швидкість відновлення даних. Використання декількох дисків допоможе швидше отримувати необхідні дані замість того, аби при виконанні роботи покладатися лише на один диск. Рішення RAID може бути апаратним і програмним. Наступні властивості описують, як RAID зберігає дані на різних дисках: парність – виявлення помилок даних; чергування – запис даних на декількох дисках; віддзеркалення – зберігання дублікатів даних на іншому диску.

Актуальною рекомендацією кібербезпеки та захисту персональних даних користувачів СДН ВВНЗ є використання Spanning Tree – мережевого протоколу, що забезпечує надмірність. Основна функція STP полягає в тому, щоб запобігти зацикленню трафіка в мережі, коли між комутаторами

існує декілька з’єднань. STP гарантує, що надмірні фізичні канали не мають петель. Це гарантує наявність лише одного логічного шляху між усіма пунктами призначення в мережі. STP навмисно блокує резервні шляхи, які можуть спричинити петлі.

Доцільно звернути увагу на те, що шлюз за замовчуванням зазвичай є маршрутизатором, який забезпечує доступ до іншої частини мережі або до Інтернету. Якщо функції шлюзу за замовчуванням виконує один маршрутизатор, він потенційно стає єдиною точкою відмови. Надлишковість маршрутизатора передбачає: вибір установки додаткового резервного маршрутизатора; здатність мережі динамічне відновлюватися після відмови пристрою, який виконує функції шлюзу, відома як надлишковість першого кроку. Тому надлишковість маршрутизатора також є актуальною рекомендацією кібербезпеки та захисту персональних даних користувачів СДН ВВНЗ. Параметри надлишковості маршрутизаторів – варіанти для забезпечення надлишковості маршрутизаторів включають:

Hot Standby Router Protocol – протокол гарантує високу доступність мережі, забезпечуючи надлишковість маршрутизації першого кроку;

Virtual Router Redundancy Protocol (VRRP) – маршрутизатор VRRP запускає протокол VRRP один або разом з декількома іншими маршрутизаторами, підключеними до локальної мережі. У конфігурації VRRP вибраний маршрутизатор є головним віртуальним маршрутизатором, а інші маршрутизаторами є запасними на випадок відмови головного виртуального маршрутизатора;

Gateway Load Balancing Protocol – протокол який захищає трафік даних від відмов маршрутизатора або мережі, подібно до HSRP і VRRP, а також дозволяє балансувати навантаження між групою резервних маршрутизаторів;

Резервне розміщення – ВВНЗ може знадобитись резервне розташування в залежності від її потреб. Як відоме існують три форми

розміщення резервів. Забезпечення синхронізації обидва місця розташування в реальному часі, вимагає високої пропускної здатності і близькості розташування для зменшення затримок.

Контроль доступу до файлів в ВВНЗ та забезпеченні дозволів, що обмежують доступ до папки або файлу для окремої особи або для групи користувачів СДН.

Також доцільно *забезпечити шифрування файлів.* Як відомо, шифрування – це інструмент, який використовується для захисту даних. Шифрування перетворює дані з використанням складного алгоритму, щоб зробити їх нечитабельними. Програми можуть шифрувати файли, папки і навіть цілі диски.

Створення процедури резервного копіювання системи і даних. Резервне копіювання даних зберігає копію інформації з комп’ютера на знімний носій резервного копіювання. Резервне копіювання даних є одним з найбільш ефективних способів захисту від втрати даних. Якщо комп’ютерне обладнання виходить з ладу, користувач може відновити дані з резервної копії, як тільки система буде працювати.

Цілком логічною та ефективною є рекомендації щодо фільтрації і блокуванню контенту, клонування диску та використання утиліти Deep Freeze. Фільтрація і блокування контенту важливе для забезпечення контролю вмісту з метою обмеження доступ користувача до певного вмісту веб-браузера через Інтернет. Програми контролю вмісту повинні блокувати сайти, які містять певні типи матеріалів. Можна вважати цю рекомендацію другорядною для забезпечення захисту персональних даних.

Багато сторонніх додатків доступно для відновлення системи до стану за замовчуванням. Це дозволяє адміністратору захищати операційну систему і конфігураційні файли системи. Клонування диска копіює вміст жорсткого диска комп’ютера в файл образу. Утиліта Deep Freeze «заморожує» розділ жорсткого диска. У випадку коли користувач СДН

перезавантажує систему, система повертається до «замороженої» конфігурації. Система не зберігає ніяких змін, внесених користувачем, тому будь-які зміни, встановлені програми або збережені файли, втрачаються при перезапуску системи.

Фізичний захист комп'ютерної техніки – тривіальні, але ефективні заходи: використання кабельних замків для обладнання; забезпечення кімнати с телекомунікаціями зачиненими; використання захисної клітки навколо обладнання.

Реалізація таймеру виходу з системи доцільна так, як у випадку коли співробітник встає на перерву і залишає свій комп'ютер, то будь-яка інформація про цю систему стає доступною для неавторизованого користувача. Тайм-аут очікування і блокування екрану також є способом захисту. Співробітники можуть вийти або ні зі свого комп'ютера, коли вони покидають робоче місце. Тому найкраще налаштувати таймер простою, після спрацювання якого користувач автоматично виходить із системи, а екран блокується.

Адміністраторам СДН у ВВНЗ доцільне контролювати час входу в систему, наприклад, щоб співробітники аутентифікувалися в системі в певні години. Система блокує логіни входу за межами вказаного інтервалу часу. Використання відстеження GPS – стандартна функція на смартфонах і забезпечує відстеження місця розташування в реальному часі. Інвентаризація та RFID-мітки. Радіочастотна ідентифікація (Radio frequency identification, RFID) використовує радіохвилі для ідентифікації та відстеження об'єктів. Системи інвентаризації використовує RFID-мітки, прикріплені до всіх предметів, які організація хоче відстежувати.

4.2. Комп’ютерне моделювання елементів захисту системи дистанційного навчання

Модельний приклад № 1. В прикладі моделювання методу прогнозування, який описано в розділі 3, параметри моделі були прийняті за замовчуванням. Але використання процедури субтрактивної кластеризації з самого початку повинно оптимізувати модель за точністю та використанням обчислювальних ресурсів. Приведемо результати відповідного дослідження.

Будемо використовувати навчальні дані з файлу data_shapran_2.dat (рис. 3.2). При визначенні режиму налаштування типу функцій належності та кількості термів скористаємось моделлю субтрактивної кластеризації (рис. 4.1). Нагадаємо про те, що задача нечіткої кластеризації полягає у визначенні об’єктивного розбиття даних на класи незалежно від суб’єктивного судження дослідника. Відомо, що особливістю процедур кластеризації є їх використання в умовах відсутності якої-небудь інформації про закони розподілу даних.

Рис. 4.1. Метод субтрактивної кластеризации

На відміну від прикладу, описаного в розділі 3, отримана наступна характеристика кількості термів вхідних змінних (рис.4.2)

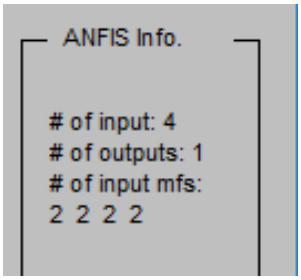


Рис. 4.2. Кількість термів вхідних змінних

Відповідна структура ANFIS наведена на рис. 4.3.

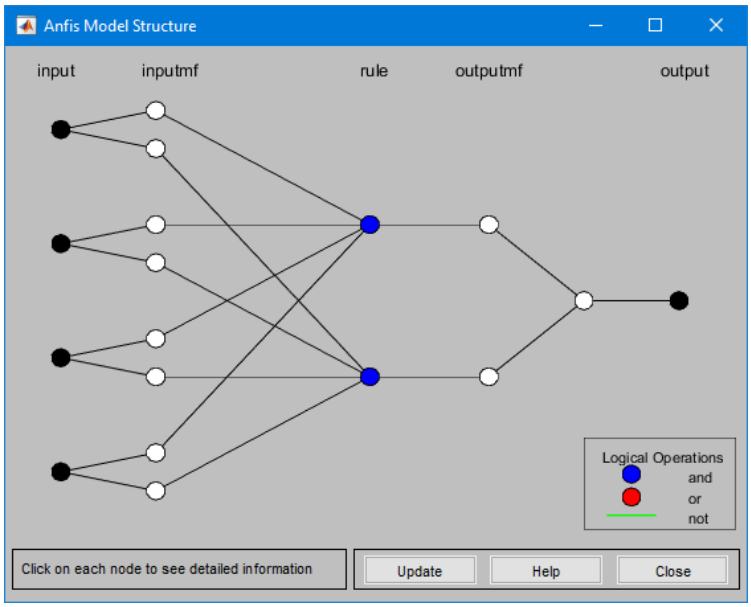


Рис. 4.3. Структура ANFIS

Виконано навчання нейронної мережі гібридним методом з налаштуванням рівня похибки та кількості циклів навчання, як показано на рис.4.4.

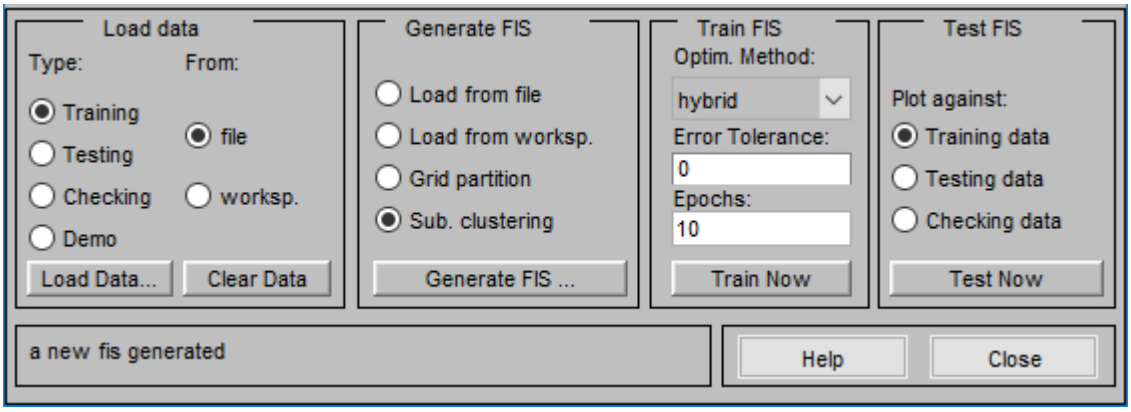


Рис. 4.4. Параметри рівня похибки та кількості циклів навчання

Результати навчання нейронної мережі та структура її правил зображені на рис.4.5.

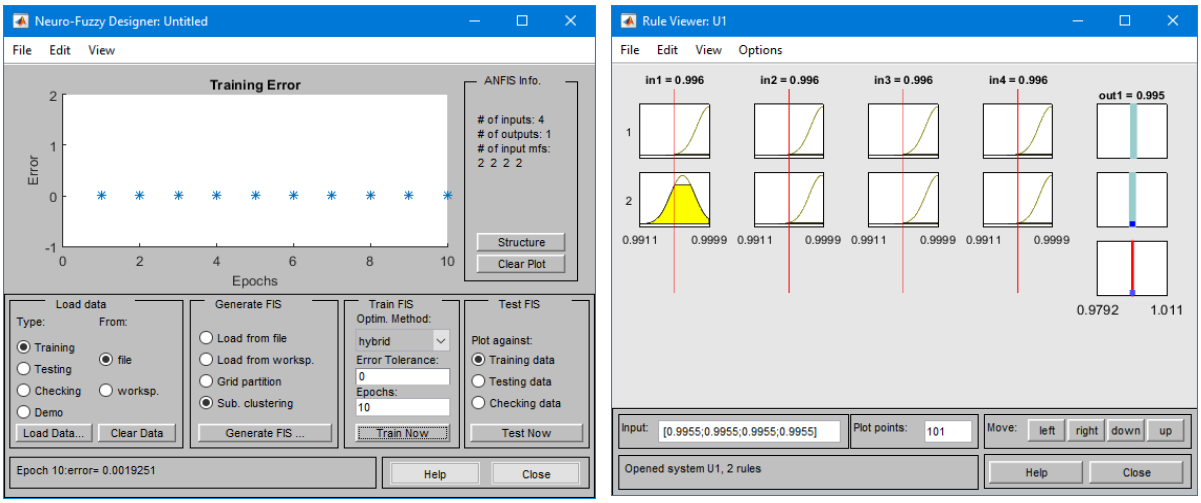


Рис. 4.5. Результати навчання нейронної мережі та структура її правил

Отже, за результатами моделювання можна з упевненістю сказати те, що використання субтрактивної кластеризації при визначенні режиму налаштування типу функцій належності та кількості термів не надало бажаного приросту точності. Це пояснюється спрощенням правил нечіткого логічного виведення, та, як наслідок, – погіршенням точності прогнозу.

Результати дослідження методів навчання нейронної мережі ANFIS (рис. 4.6) визначили перевагу гібридного методу в порівнянні з методом зворотного розповсюдження.

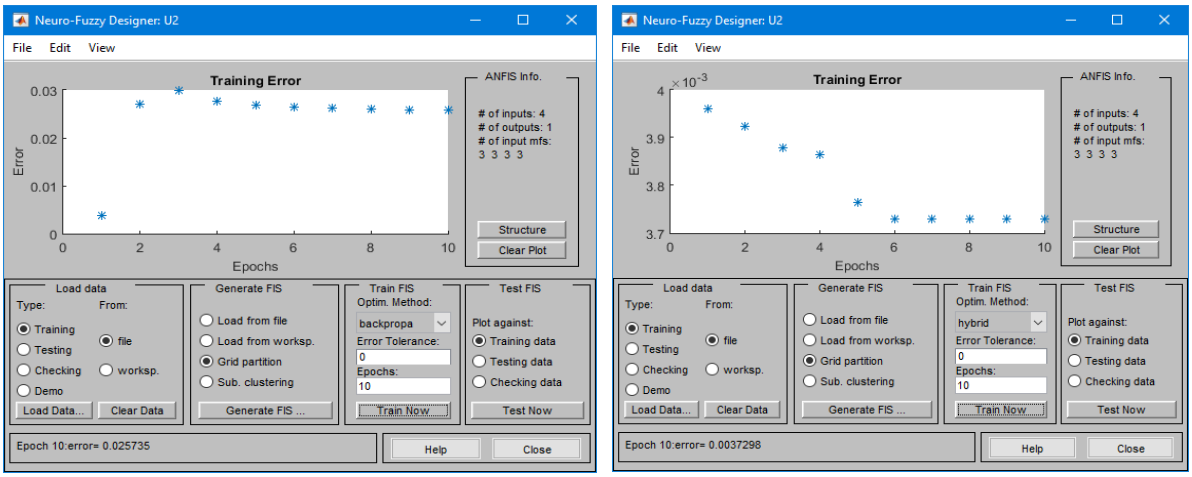
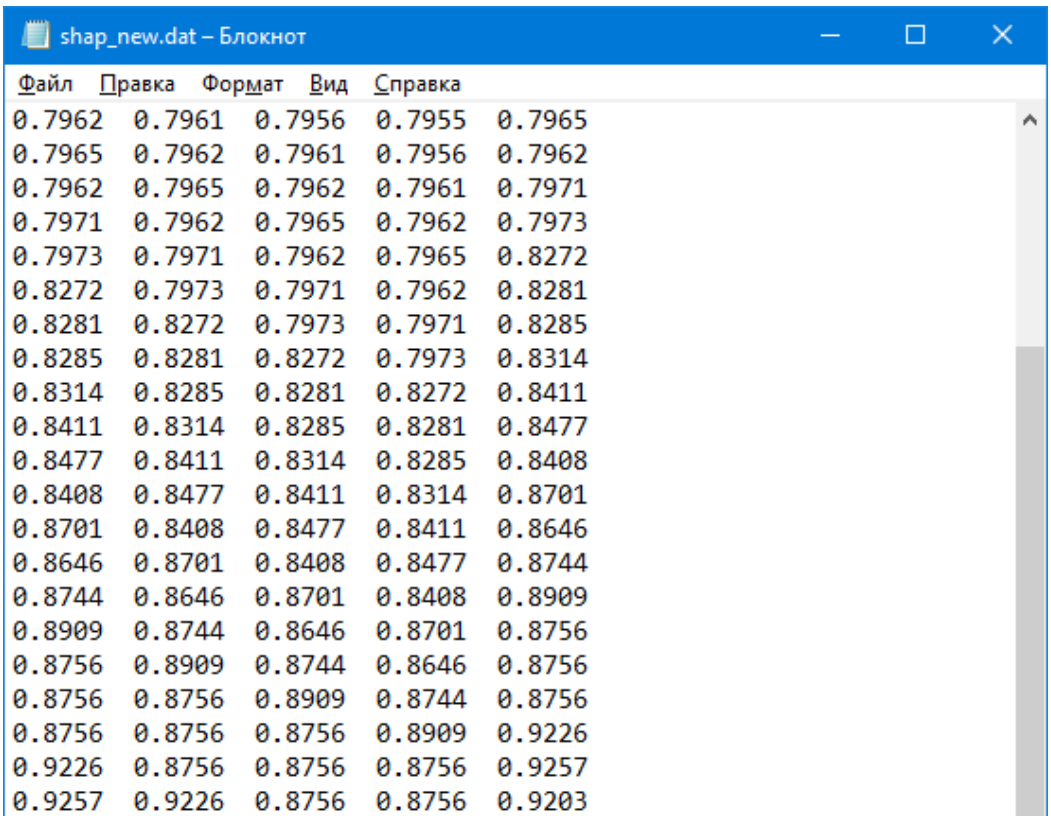


Рис. 4.6. Результати дослідження методів навчання нейронної мережі

Модельний приклад № 2. Аналіз рівня захищеності персональних даних користувачів ДН, які наведені в табл. 2.10, дозволяє зробити висновок про те, що фактичне значення показника ефективності постійне високе й тому відсутня тенденція щодо його зміни. Цілком логічна думка про те, що адекватність та точність методу прогнозу може бути пов’язана саме з відсутністю явної тенденції до зміни.

Тому для підтвердження достовірності наукового результату стосовно методу прогнозу доцільно використати експериментальні данні комплексної оцінки ефективності СДН, які були отримані за період з 01.09.2022 по 19.10.2022. Допущенням є те, що комплексна оцінка СДН виконувалася з урахуванням оцінки ефективності системи захисту персональних даних користувачів. Дані з 15.10.2022 по 19.10.2022 використані для перевірки точності моделі прогнозу. Навчальні дані мають вигляд, як на рис. 4.7.


shap_new.dat – Блокнот

Файл Правка Формат Вид Справка

0.7962	0.7961	0.7956	0.7955	0.7965
0.7965	0.7962	0.7961	0.7956	0.7962
0.7962	0.7965	0.7962	0.7961	0.7971
0.7971	0.7962	0.7965	0.7962	0.7973
0.7973	0.7971	0.7962	0.7965	0.8272
0.8272	0.7973	0.7971	0.7962	0.8281
0.8281	0.8272	0.7973	0.7971	0.8285
0.8285	0.8281	0.8272	0.7973	0.8314
0.8314	0.8285	0.8281	0.8272	0.8411
0.8411	0.8314	0.8285	0.8281	0.8477
0.8477	0.8411	0.8314	0.8285	0.8408
0.8408	0.8477	0.8411	0.8314	0.8701
0.8701	0.8408	0.8477	0.8411	0.8646
0.8646	0.8701	0.8408	0.8477	0.8744
0.8744	0.8646	0.8701	0.8408	0.8909
0.8909	0.8744	0.8646	0.8701	0.8756
0.8756	0.8909	0.8744	0.8646	0.8756
0.8756	0.8756	0.8909	0.8744	0.8756
0.8756	0.8756	0.8756	0.8909	0.9226
0.9226	0.8756	0.8756	0.8756	0.9257
0.9257	0.9226	0.8756	0.8756	0.9203

Рис. 4.7. Навчальні дані (приклад 2)

Навчальні дані та структура ANFIS представлено на рис. 4.8. На рис. 4.9 показано результати навчання та правила виведення.

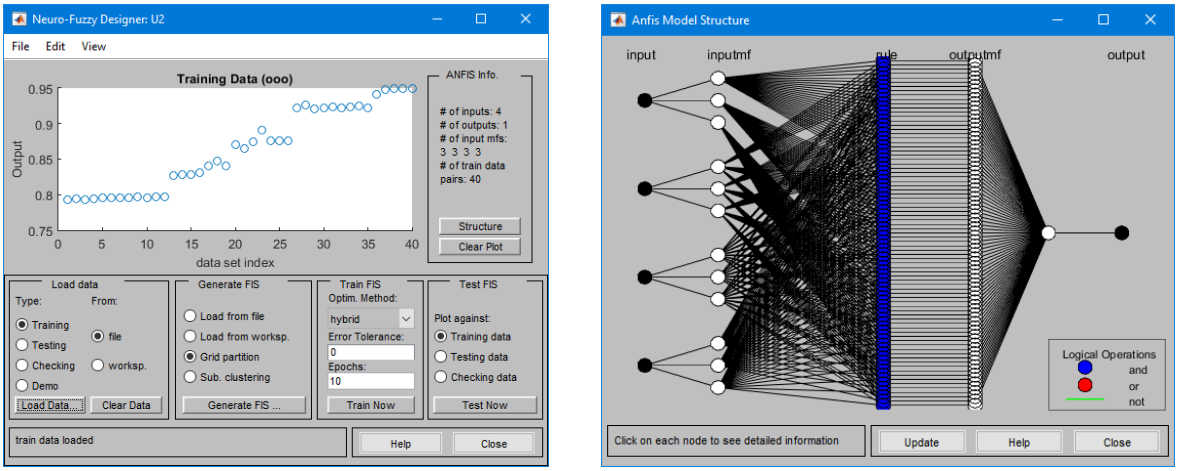


Рис. 4.8. Навчальні дані та структура ANFIS (приклад 2)

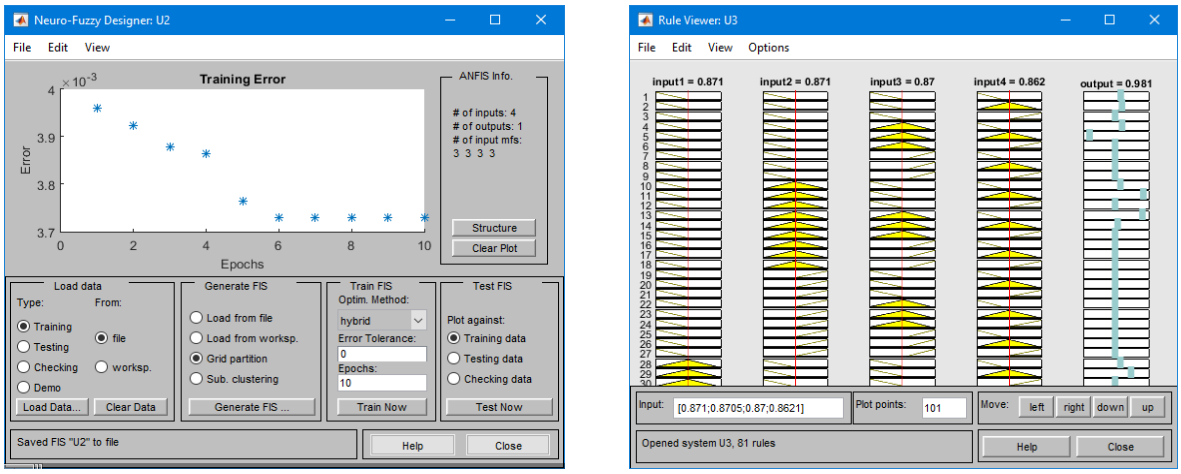


Рис. 4.9. Результати навчання та правила виведення (приклад 2)

Результати прогнозу, які отримані на основі ANFIS свідчать про збіг даних з реальними значеннями, які були обрані для перевірки адекватності та точності методу (табл. 4.1).

Таблиця 4.1

Оцінка точності прогнозу

Експеримент	**Прогноз**	**Похибка, %**
0,9548	0,9505	0,460829
0,9585	0,9544	0,438185
0,9597	0,9569	0,302178
0,9571	0,9575	0,031340
0,9611	0,9599	0,135262

Результат функції `evalfis`:

```
>> out = evalfis([  0.9493    0.9492    0.9490    0.9483;
                    0.9548    0.9493    0.9492    0.9490;
                    0.9585    0.9548    0.9493    0.9492;
                    0.9597    0.9585    0.9548    0.9493;
                    0.9598    0.9597    0.9585    0.9548],U1)
out =
           0.9505
           0.9544
           0.9569
           0.9575
           0.9599
```

Отже, середня похибка прогнозу складає ≈ 0,26 %, що ще раз підтверджує достовірність наукового результату стосовно методу прогнозування.

4.3. Дослідження ефективності методики підвищення захищеності персональних даних в системі дистанційного навчання Збройних Сил України

Аналіз конкретної системи фактично полягає у виділенні певної підсистеми з більш великої системи. Виділяючи підсистему, фактично вводяться границі, яких насправді не існує. При побудові моделей реальних явищ дослідник, бажаючи користуватися математичними методами, часто

вносить визначеність там, де її немає за існуючими умовами. Особливо небезпечним є використання штучної визначеності при управлінні.

Інформація про СДН носить суб’єктивний характер і містить велику кількість невизначеностей типу "багато", "мало", "сильно", "слабко", "високий", "низький" тощо, які не мають аналогів у мові традиційної математики. За глибоко вкоріненою традицією наукове мислення розуміння явища, на жаль, ототожнюється з можливістю його кількісного аналізу.

Наявність математичних засобів відображення нечіткості вихідної інформації дозволило побудувати модель, адекватну реальності.

Мова традиційної математики, що спирається на теорію множин і двозначну логіку, виявляється недостатньо гнучкою для моделювання реальних складних систем, оскільки в ній немає засобів описання понять, якими користується людина і які мають невизначений сенс.

Одна з основних цілей побудови математичних моделей систем – обробка наявної інформації для вибору раціонального (оптимального) варіанта управління системою. Для систем, складність яких перевищує деякий пороговий рівень, точність і практичний сенс стають практично виключними один для одного характеристиками.

У зв’язку з цим до початку дисертаційного дослідження загальна оцінка стану системи дистанційного навчання ЗСУ не проводилась, а реагування на загрози відбувалось на основі моніторингу подій з подальшим усуненням виявлених вразливостей та порушень.

Тому запропоновано удосконалену модель оцінки стану системи захисту персональних даних, яка базується на нечіткому логічному виведенні.

В рамках дисертаційного дослідження проведено науковий експеримент щодо визначення оцінки стану системи захисту персональних даних користувачів системи дистанційного навчання ЗС України на основі моделі, яка запропонована в якості другого наукового результату

дослідження. Експеримент проводився з 1 квітня 2022 року по 30 червня 2023 року.

Для порівняння аналізувались два часові періоди: 2022 рік та 2023 рік.

В якості експертів до експерименту були залучені 32 співробітника організацій, які беруть участь в забезпеченні роботи системи дистанційного навчання ЗС України. А саме, 5 співробітників наукового центру дистанційного навчання Національного університету оборони України, 6 інженерів організації, яка надає послуги хостингу, адміністрування серверів та мережі Інтернет, 3 співробітника відділу зв'язку та інформаційних систем Національного університету оборони України, 5 співробітників підрозділу кіберзахисту Міністерства оборони України, 2 співробітника центру імітаційного моделювання Національного університету оборони України, які залучені до системного адміністрування серверів та мереж університету і 11 осіб, які виконують функції локальних адміністраторів баз даних персональних даних користувачів системи дистанційного навчання ЗСУ у своїх організаціях.

Оцінювання проводилось щоденно наприкінці робочого дня відповідно до моделі, запропонованої в якості другого наукового результату дисертаціного дослідження. Результати подавались для узагальнення та опрацювання засобами Google Forms.

Застосування у 2023 році методу прогнозування стану системи захисту персональних даних користувачів СДН ЗСУ дозволило вчасно виявляти характер тенденцій до змін оцінки стану зазначеної системи та оперативно реагувати.

Для визначення ефективності розроблених наукових результатів аналізуються показники, які характеризують рівень ризику, що виник у зв'язку з падінням рівня захищеності персональних даних користувачів СДН Збройних Сил України на певному часовому проміжку.

Серед численних факторів, які впливали на оцінки експертів, відзначені наступні:

вірусні атаки та поява нових вірусів;

оновлення антивірусних баз;

оновлення програмного забезпечення за напрямами діяльності, обслуговування та оновлення апаратного забезпечення;

організація резервного копіювання та інші заходи системного адміністрування;

намагання злому облікових записів та несанкціонованого доступу;

спроби злому веб-серверів та серверів баз даних;

підвищення навантажень на ресурси;

активність ботів;

проблеми електропостачання;

збільшення помилок користувачів;

порушення політики безпеки;

поява великої кількості нових користувачів та випуск попередніх;

підвищення активності користувачів у зв’язку зі збільшенням частки освітнього процесу з використанням технологій дистанційного навчання;

розроблення та впровадження нових компонентів прикладного програмного забезпечення;

результати моніторингу системи дистанційного навчання, мережі, серверів;

заплановані планові заходи розвитку та підтримки системи дистанціного навчання та інші.

На рис. 4.10 показаний графік функції залежності оцінки стану системи захисту ПДК ЗСУ від часу у 2022 та 2023 роках.

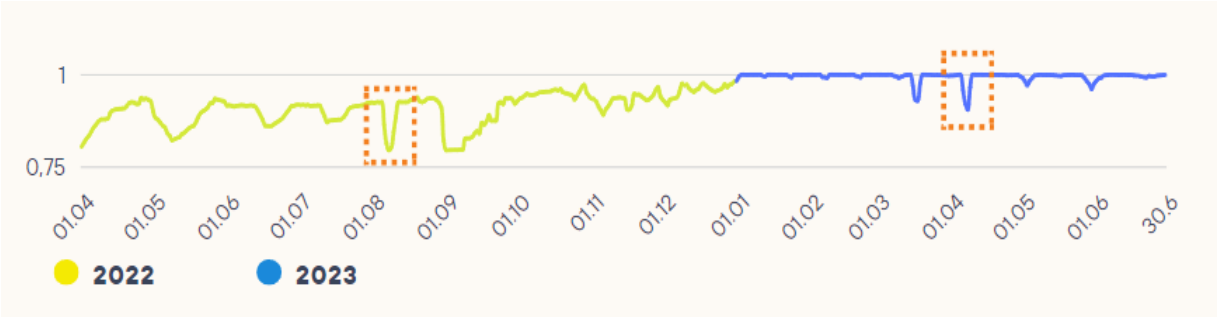


Рис. 4.10. Графік функції залежності оцінки стану системи захисту ПДК ЗСУ від часу (діб) у 2022 та 2023 роках

Зазначимо, що у 2023 році підвищився загальний рівень оцінки стану системи захисту ПДК ЗСУ та зменшилась частота коливання рівня оцінки стану системи, абсолютне скорочення рівня та час відновлення до попереднього рівня. Викривлення графіків пов’язані з інтегральним впливом численних факторів, зазначених вище, в певні часові періоди і заходами реагування на них. За даними експертів провали рівня оцінки стану системи захисту ПДК ЗСУ у травні, червні та липні 2022 року насамперед пов’язані з активними російськими ворожими хакерськими атаками на українські ресурси, а саме DDoS атаки, численними брутфорс (Brute force) атаками та намаганнями скористатись виявленими вразливостями компонентів LMS та CMS. За сигнатурами шкідливого програмного забезпечення найпоширенішими були: Backdoor:PHP/Remoteshell.V, Exploit:O97M/CVE-2017-11882.PK!MTB, Backdoor:PHP/OrbWS!rfn, Exploit:O97M/CVE-2017-11882.SZTG!MTB та TrojanDownloader:O97M/Emotet.RPL!MTB. Але, варто зазначити, що це лише основні, але не єдині фактори, які мали вплив в ті періоди часу на скорочення рівня захищеності персональних даних користувачів.

У вересні 2022 року окрім зазначених вище факторів вагомий вплив мало різке збільшення нових користувачів, виникнення проблем з електропостачанням, збільшення частки занять з використанням технологій дистанційного навчання та оновленням програмного забезпечення, що

відповідно має вагомий вплив на велику кількість процесів забезпечення захищеності ПДК СДН ЗСУ.

У 2023 році були спроби повторити DDoS атаки та використати вразливості компонентів програмного забезпечення.

Встановлено, що у 2022 році серед періодів падіння оцінки стану системи захисту персональних даних користувачів СДН ЗСУ максимальний рівень падіння був в період з 5 по 12 серпня 2022 року з показника 0,9257 до 0,7955, тобто на 0,1302. Час, за який відбулось падіння, реагування і повернення на попередній високий рівень склав 168 годин. У 2023 році серед періодів падіння оцінки стану системи захисту персональних даних користувачів СДН ЗСУ максимальний рівень був в періоді з 5 по 10 квітня 2023 року, де відбулось падіння з показника 0,9999 до 0,9051, тобто на 0,0948. Час реагування та повернення на попередній рівень склав 120 годин.

На рис. 4.11 показано порівняння графіків функцій залежності оцінки стану системи захисту ПДК ЗСУ від часу у зазначених періодах 2022 та 2023 років:

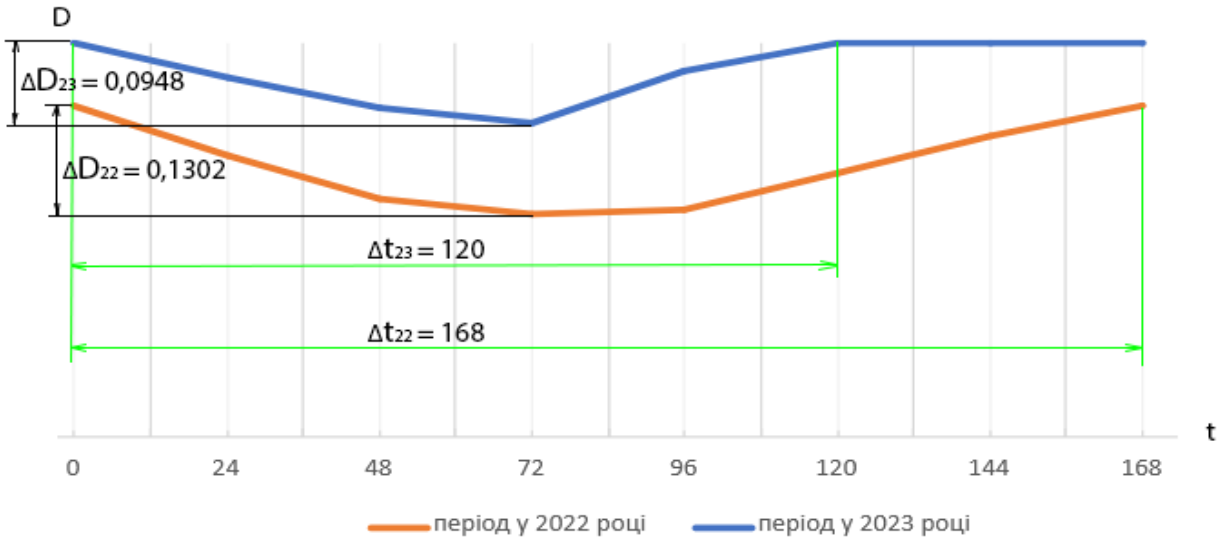


Рис. 4.11. Порівняння графіків функцій обраних критичних періодів залежності оцінки стану системи захисту ПДК ЗСУ від часу (годин) у 2022 та 2023 роках

Відповідно до розрахунків:

(0,1302 – 0,0948)/0,1302 = 0,2719

(168 - 120)/168 = 0,2857.

Це показує, що впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилась на 26-28%, а час реагування на загрози захищеності даних зменшився на 28-30%. Що ще раз підтверджує досягнення мети наукового дослідження.

Висновки до розділу 4

1. Реалізація політики та стратегії кібербезпеки для захисту персональних даних користувачів СДН забезпечується шляхом застосування відповідних способів, засобів та процедур. Тому методика підвищення захищеності персональних даних та наукові результати, які розроблене з метою її деталізації фактично вирішує завдання управління безпекою. Отже, практичні рекомендації стосуються саме цього та перш за все спрямовані на використання відповідних міжнародних стандартів з цього напряму, наприклад, стандарту ISO/IEC 27000, який є універсальною структурою для кожного типу організації.

2. Рекомендації поєднують технології захисту на основі програмного забезпечення для захисту операційних системи, баз даних та інші служби, що працюють на робочих станціях користувачів СДН, портативних пристроях і серверах; апаратні засоби захисту, які мають у складі пристрої

брандмауера, системи виявлення вторгнень, системи захисту від вторгнення (IPS) та системи фільтрації вмісту; мережеві технології захисту.

3. Рекомендації щодо контролю цілісності даних полягають у використанні хешування – процедури, яка забезпечує цілісність даних, беручи двійкові дані (повідомлення) і створюючи з них вихідне значення фіксованої довжини, що називається хеш-значенням або дайджестом повідомлення.

4. Забезпечення надлишковості залишається актуальною рекомендацією кібербезпеки та захисту персональних даних користувачів СДН ВВНЗ. Це обумовлено необхідністю виявлення та виправлення так званої єдиної точки відмови. Одиничною точкою відмови може бути конкретна частина апаратного забезпечення, процес, конкретний фрагмент даних або навіть найважливіша утиліта. Точки відмови – це слабкі ланки ланцюга, які можуть спричинити збій у роботі центру ДН.

5. Для вирішення проблеми єдиної точки відмови потрібно змінити критичну операцію так, щоб вона не покладалася лише на один елемент. При виконанні критичних операцій ВВНЗ може вбудовувати резервні компоненти, які б могли взяти на себе процес, якщо одна з цих точок відмовить.

6. Багато сторонніх додатків доступно для відновлення системи до стану за замовчуванням. Це дозволяє адміністратору захищати операційну систему і конфігураційні файли системи. Клонування диска копіює вміст жорсткого диска комп’ютера в файл образу. Утиліта Deep Freeze «заморожує» розділ жорсткого диска. У випадку коли користувач СДН перезавантажує систему, система повертається до «замороженої» конфігурації. Система не зберігає ніяких змін, внесених користувачем, тому будь-які зміни, встановлені програми або збережені файли, втрачаються при перезапуску системи.

7. Рекомендації щодо фізичного захисту комп’ютерної техніки є тривіальні, але ефективні: використання кабельних замків для обладнання; забезпечення кімнати з телекомунікаціями зачиненими; використання захисної клітки навколо обладнання. Реалізація таймеру виходу з системи доцільна так, як у випадку коли співробітник встає на перерву і залишає свій комп’ютер, то будь-яка інформація про цю систему стає доступною для неавторизованого користувача. Тайм-аут очікування і блокування екрану також є способом захисту. Співробітники можуть вийти або ні зі свого комп’ютера, коли вони покидають робоче місце. Тому найкраще налаштувати таймер простою, після спрацювання якого користувач автоматично виходить із системи, а екран блокується.

8. Адміністраторам СДН у ВВНЗ доцільно контролювати час входу в систему, наприклад, щоб співробітники аутентифікувалися в системі в певні години. Система блокує логіни входу за межами вказаного інтервалу часу. Використання відстеження GPS – стандартна функція на смартфонах і забезпечує відстеження місця розташування користувача в реальному часі. Радіочастотна ідентифікація (Radio frequency identification, RFID) використовує радіохвилі для ідентифікації та відстеження об’єктів. Системи інвентаризації використовує RFID-мітки, прикріплені до всіх предметів, які організація хоче відстежувати.

9. Аналіз рівня захищеності персональних даних користувачів СДН, яких представлений в табл. 2.10 дозволяє зробити висновок, що фактичне значення показника ефективності постійне високе та відсутня тенденція його зміни. Тому для підтвердження достовірності наукового результату стосовно методу прогнозу доцільно використовувати експериментальні дані комплексної оцінки ефективності СДН. Комплексна оцінка СДН виконувалася з урахуванням оцінки ефективності системи захисту персональних даних користувачів. Для перевірки точності моделі прогнозу були використані дані контрольної вибірки (з 15.10.2022 по 19.10.2022).

Результати прогнозу, які отримані на основі ANFIS свідчать про збіг даних з реальними значеннями, які були обрані для перевірки адекватності та точності методу. Середня похибка прогнозу складає $\approx 0{,}26\ \%$, що підтверджує достовірність наукового результату стосовно методу прогнозування стану системи захисту.

10. Впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилась на 26-28%, а час реагування на загрози захищеності даних зменшився на 28-30%. Що ще раз підтверджує досягнення мети наукового дослідження.

ВИСНОВКИ

В результаті дисертаційних досліджень, виконаних автором, вирішено нове актуальне наукове завдання удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України на основі штучного інтелекту. Дане наукове завдання має важливе значення для теорії і практики підвищення якості освітнього процесу у вищих військових навчальних закладах та закладах вищої освіти, підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України та для розвитку сучасної політики та стратегії інформаційної або кібербезпеки інформаційного освітнього середовища в цілому. Відсутність аналогічних рішень в нашій країні і за кордоном робить результати досліджень пріоритетними.

В дисертаційному дослідженні отримані такі основні результати:

1. На підставі проведеного аналізу встановлено, що на теперішній час рівень ефективності, показники якості та вартості систем дистанційного навчання навчальних закладів Збройних Сил України продовжують покращуватися. При цьому, особлива увага приділяється саме заходам кібербезпеки, а саме, забезпеченню захищеності персональних даних користувачів системи дистанційного навчання. Даний напрям розвитку відповідає вимогам законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Встановлено, що існуюча стратегія кібербезпеки зосереджена в основному на моніторингу загроз і захисті від них. Перспективна стратегія кібербезпеки має бути спрямована на оцінку та зменшення ризиків, що дозволяє уникнути фрагментів програмного коду або послідовності команд, що використовують вразливості в програмному

забезпеченні, які можуть завдати шкоди. Ці зміни створюють абсолютно нові тенденції, які пов’язані з використанням штучного інтелекту. Таким чином, для вирішення проблеми забезпечення кібербезпеки системи дистанційного навчання закладів Збройних Сил України актуальним є наукове завдання удосконалення існуючих та розробки нових моделей та методів підвищення захищеності персональних даних користувачів системи дистанційного навчання ЗС України на основі штучного інтелекту.

2. Вперше запропонована методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України, яка забезпечує своєчасне реагування на потік загроз та базується на основі впровадження моделей та методів нечіткої логіки та гібридних мереж. Методика поєднує моделі та методи, які спрямовані на комплексне вирішення наступних завдань: 1) ідентифікація загрози та визначення стану системи захисту персональних даних, а саме, система забезпечує захист в повному обсязі або не забезпечує захист та вимагає застосування способів та засобів, які раніше не були використані; 2) формування відповідної протидії на загрозу з арсеналу існуючих методів, способів, засобів та процедур або, у випадку їх непридатності, формування стратегії їх удосконалення та розробки нових; 3) прогнозування стану системи захисту в майбутньому з метою попередження шкідливого впливу загроз. Практична реалізація методики дозволяє забезпечити постійний захист персональних даних користувачів системи дистанційного навчання Збройних Сил України;

3. Удосконалено модель оцінки стану системи захисту персональних даних, яка на відміну від існуючих базується на нечіткому логічному виведенні (алгоритм Мамдані). В моделі забезпечено оптимальний метод дефазифікації, раціональна вага та кількість правил, оптимальні параметри функцій належності. Застосування методики дозволяє отримувати кількісну

оцінку ефективності системи, яка необхідна для прийняття рішення щодо подальшого її удосконалення;

4. Вперше запропоновано метод прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз, який побудований на основі технології адаптивної нейронної нечіткої мережевої системи виведення ANFIS (Adaptive Neuro-Fuzzy Inference System). Використання методу дозволяє прогнозувати ефективність системи захисту та планувати заходи щодо забезпечення підвищення захищеності персональних даних. За результатами перевірки середня похибка прогнозу 0,006 ÷ 0,26 %.

5. Практичне значення одержаних результатів полягає в тому, що їх реалізація доцільна в математичному та програмному забезпеченні, як складової системи управління захистом персональних даних. Впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилась на 26-28%, а час реагування на загрози захищеності даних зменшився на 28-30%. Що ще раз підтверджує досягнення мети наукового дослідження.

6. Мета дослідження, яка полягає підвищенні захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України досягнута і всі окремі завдання вирішені повністю. Наукові результати досліджень є внеском в розвиток наукових основ підвищення захищеності персональних даних користувачів системи дистанційного навчання, а також внеском в теорію штучного інтелекту в контексті кібербезпеки системи дистанційного навчання Збройних Сил України.

7. Результати дисертаційних досліджень реалізовані в освітньому процесі Національного університету оборони України. Реалізацією

отриманих результатів є розроблені методичні рекомендації щодо підвищення ефективності функціонування системи дистанційного навчання в Збройних Силах України, методичні рекомендації щодо реалізації онлайн-курсу розвитку цифрової компетентності користувачів системи дистанційного навчання Збройних Сил України та окремі навчальні питання методичної розробки “Курсу підвищення кваліфікації наукових і науково-педагогічних працівників вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти з питань організації та використання технологій дистанційного навчання в Збройних Силах України”, акти реалізації № 609/10/268 від 26.09.2023 р. та № 609/10/269 від 26.09.2023 р.

8. Напрямки подальших досліджень полягають у комплексному вирішенні проблеми кібербезпеки як системи дистанційного навчання, так і інформаційного середовища вищих військових навчальних закладів Збройних Сил України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2016, – 340 с.

2. Бурячок В.Л., Толюпа С.В., Аносов А.О. Системний аналіз та прийняття рішень в інформаційній безпеці. – К. : ДУТ, 2015. –345 с.

3. Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби. К.: ТОВ "Наш формат", 2016. – 176с.

4. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці. – К.:ДУТ, 2015. – 345 с.

5. Виявлення та блокування повільних DDOS-атак за допомогою прогнозування поведінки користувача / О.А. Лаптєв, С.С. Бучик, В.А. Савченко, В.С. Наконечний, І.І. Михальчук, Я.В. Шестак // Наукоємні технології. Інформаційні технології, кібербезпека. НАУ. Vol. 55 No 3. 2022. – С. 184-192.

6. Голев Д.В., Кононович В.Г., Хомич С.В. Методики оцінки інформаційної захищеності телекомунікацій: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 218 с.

7. Гринь А. К., Довгань О. Д., Журавель В. І. Менеджмент інформаційної безпеки. – К.: Наук.-вид. центр НА СБ України, 2013. – 456 с.

8. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки.– К.: Видавництво НА СБ України, 2021. – 256 с.

9. Дуравкін Е.В., Толюпа С.В., Лукова-Чуйко Н.В. Захист інформації в інформаційно-комунікаційних системах. Лабораторний практикум. – К.:. Інститут обдарованої дитини НАПН України, 2015. – 174с.

10. Закон України «Про захист персональних даних» від 1 червня 2010 року. http://zakon0.rada.gov.ua/laws/show/2297-17 (дата звернення: 10.05.2023).

11. Зайченко Ю. П. Нечіткі моделі й методи в інтелектуальних системах. – К.: Видавничий дім «Слово», 2008. – 344 с.

12. Інформаційна безпека / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2016. – 352 с.

13. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Харків: Вид. ХНЕУ, 2013. – 364 с.

14. Кирик В. В. Комп'ютерно-інтегровані технології управління на основі нечіткої логіки. Акад. муніцип. управління. – К:, 2008, – 198 с.

15. Клебанова Т.С., Чаговець Л.О., Панасенко О.В. Нечітка логіка та нейронні мережі в управлінні підприємством. – Харків: ВД «ІНЖЕК», 2011. – 240 с.

16. Колодчак О. М. Сучасні методи виявлення аномалій в системах виявлення вторгнень. Вісник Національного ун–ту «Львівська політехніка». Комп'ютерні системи та мережі. № 745, 2012, С. 98–104.

17. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року, ратифікованою Верховною Радою України 6 липня 2010 року. http://zakon1.rada.gov.ua/laws/show/994_326 (дата звернення: 10.05.2023).

18. Кондратенко Ю.П., Сіденко Є.В. Нечіткі множини та нечітка логіка. Методичні рекомендації та вказівки для виконання лабораторних робіт студентами спеціальності 122 «Комп'ютерні науки». – Миколаїв : ЧНУ ім. Петра Могили, 2019. 36 с.

19. Кононюк А.Ю. Нейронні мережі і генетичні алгоритми. – К.: Корнейчук, 2008, 446 с.

20. Конституція України. http://zakon4.rada.gov.ua/.../show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.05.2023).

21. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. – К. : Центр навч.-наук, та наук.-пр. видань НА СБ України, 2014. – 190 с.

22. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, – К.: ЦП «Компринт», 2017. – 435 с.

23. Леоненков А.В. Нечёткое моделирование в среде MATLAB. – СПб : БХВ-Петербург, 2003. – 736 с.

24. Матвійчук А. В. Штучний інтелект в економіці: нейронні мережі, нечітка логіка: Монографія. – К.: КНЕУ, 2011, – 439 с.

25. Моделювання та оптимізація інформаційних систем в судноводінні / Кравченко Ю.В. та ін., за ред. О.М. Тимощук. – К. :ДУІТ, 2019, 312 с.

26. Оксіюк О.Г., Толюпа С. В., Бурячок В.Л., Вялкова В.І. Захист об’єктів інформаційної діяльності. – К.: ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка, 2018, – 322 с.

27. Положення про дистанційне навчання в Національному університеті оборони України імені Івана Черняховського, 2017, 9 с. https://adl.nuou.org.ua/storage/regulations/0f668b99a709ac012adec59958a94a10.pdf (дата звернення: 10.05.2023).

28. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних. http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 10.05.2023).

29. Прохорова О. М., Кальчук Н. В. Моделі і методи нечіткої логіки: навч. посіб. [Рукопис] Нац. аерокомс. ун-т ім. Н. Є. Жуковського “ХАІ”. – Х., 2021, – 166 с.

30. Разживін О. В., Суботін О. В. Синтез нечітких регуляторів в системах автоматичного керування. – Краматорськ : ЦТРІ «Друкарський дім», 2017, – 212 с.

31. Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г. Бекетова, Б. Ахметов, О. Корченко, В. Лахно // Безпека інформації. К : НАУ, 2016. Т. 22, № 3. С. 242–254.

32. Ротштейн О.П. Інтелектуальні технології ідентифікації: нечітка логіка, генетичні алгоритми, нейронні мережі. – Винница: УНІВЕРСУМ – Вінниця, 1999. – 320 с.

33. Ротштейн О.П., Штовба С.Д. Проектування нечітких баз знань. – Вінниця: ВДТУ, 1999, – 63 с

34. Руденко О. Г., Бодянський Є. В. Штучні нейронні мережі. – Харків: ТОВ "Компанія СМІТ", 2006. – 404 с.

35. Савченко В.А. Мультиагентна технологія пошуку цифрових радіозакладних пристроїв на основі кластеризації за методом бджолиної колонії / Савченко В.А., Савченко В.В., Мацько О.А., Кізяк Я.О., Лаптєв О.А., Лазаренко С.В. // Захист інформації, Том 21, №3, липень-вересень 2019. – С. 194–202.

36. Савченко В.А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Савченко В.А., Савченко В.В., Довбешко С.В., Мацько О.Й., Зідан А.М. // Сучасний захист інформації №4(36), 2018, – С. 40-49.

37. Савченко В.А., Боярчук Р.М., Мацько О.Й., Новікова І.В. Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз. Сучасний захист інформації. №1(41), 2020, – С. 6–10.

38. Савченко В.А., Лаптєв О.А., Кітура О.В. Виявлення інсайдерських загроз на основі інтелектуального аналізу журналів активності користувачів. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021р.). [Електронне видання]. – К. : НА СБУ, 2021. – С. 220–222.

39. Савченко В.А., Лаптєв О.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об’єктах інформаційної діяльності. – К.: ДУТ, 2020, – 126 с.

40. Савченко В.А., Мацько О.Й. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу. Сучасний захист інформації. №2(38), 2019, – С. 6-16.

41. Савченко В.А., Мацько О.Й., Пшоннік В.О. Нейромережева технологія управління багатомашинним роботизованим комплексом пошуку нелегальних випромінювачів. Сучасний захист інформації. №3(39), 2019. – С. 15-22.

42. Савченко В.А., Мельник Я.В. Підвищення надійності сучасних гетерогенних мереж з допомогою теорії перколяції. "Інфраструктура ІКТ як основа цифрової економіки". Семінар-практикум МСЕ, Київ, 14-16 травня 2019 р. – К.: ДУТ, 2019. – С. 41-42.

43. Савченко В.А., Пуха М.С., Панадій С.В. Компонентна модель захисту передачі даних у системі електронного урядування. Сучасний захист інформації №1(41), 2020. – С. 11-17.

44. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації №4(44), 2020. – С. 6–11.

45. Савченко В.А., Лаптєв О.А., Локалізація засобів негласного отримання інформації на основі застосуванням методу найменших квадратів. Телекомунікаційні та інформаційні технології. 2019, № 4 (65). С. 57 – 70.

46. Савченко В.А., Моделювання кібератак засобами теорії графів // В.А. Савченко, О.Й. Мацько, С.В. Легомінова, І.С. Полторак, В.В. Марченко // Сучасний захист інформації №4 (40), 2019. – С. 6-11.

47. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. – Житомир: Вид.О. О. Євенок, 2020. – 184 с.

48. Терехов В. А., Єфімов Д. В., Тюкин И. Ю. Нейромережні системи керування. – К.: – Вис. школа, 2002, –184 с.

49. Типовий порядок обробки персональних даних. http://www.ombudsman.gov.ua/.../tipovij-poryadok-obrobki (дата звернення: 10.05.2023).

50. Толубко В. Б., Бурячок В. Л., Толюпа С. В., Хорошко В. О. Інформаційна та кібербезпека: соціотехнічний аспект.– К.: ДУТ, 2015. – 288 с.

51. Толюпа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю. Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки. Наукоємні технології. – К.: НАУ, 2020. – № 4 (48). – С 470–477.

52. Толюпа С.В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз / Лукова-Чуйко Н.В., С.В. Толюпа, В.С. Наконечний, Браіловський М.М.: монографія. – К.: Формат, 2021. – 407 с.

53. Толюпа С.В., Політанський Л.Ф., Політанський Р.Л., Лісінський В.В. Управління інформаційною безпекою. – Ч.: Чернівецький національний університет імені Юрія Федьковича, 2021. – 540 с.

54. Толюпа С.В., Хорошко В.О., Хохлачова Ю.Є. Забезпечення інформаційної безпеки держави. Лабораторний практикум. – К.: ПВП “Задруга”, 2014. – 69с.

55. Толюпа С.В., Штаненко С.С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Випуск № 3. 2018р, С. 56–66.

56. Чоповський С. С. E-learning в ПТО, або не тільки Moodle-м живе сучасна освіта, 2016, 5 с. https://core.ac.uk/download/pdf/80500368.pdf (дата звернення: 10.05.2023).

57. Шапран О. Моделі підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Телекомунікаційні та інформаційні технології. № 2 (45), 2023, с. 33-45.

58. Шапран О., Махно Є. Аналіз процесів інтелектуалізації системи дистанційного навчання у Збройних силах України. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (46), 2023, с. 107-114.

59. Шапран О., Кравченко Ю., Махно Є., Тищенко М. Модель інтелектуалізації оптимальної траєкторії проходження дистанційного курсу. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (43), 2022, с.105 – 114.

60. Шапран О., Судніков Є., Тарасенко Н. Захист персональних даних методом знеособлення. Забезпечення кібероборони держави: збірник матеріалів III науково-практичного вебінару 29 вересня 2022 року м. Київ. – К.: НУОУ, 2022. – 192 с.

61. Шапран О.О., Гогонянц С.Ю., Грицай П.М. Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (34), 2019, с.29-36.

62. Шапран О.О., Гогонянц С.Ю., Клочко А.О. Технології дистанційного навчання у системі військової освіти. XXIII Міжнародна науково-практична конференція “THEORETICAL and PRACTICAL FOUNDATIONS of SOCIAL PROCESS MANAGEMENT”, 29-30 червня 2020 р., Сан-Франциско, США, 4 с.

63. Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Обґрунтування напрямку дослідження стійкості гетерогенних мереж до кібератак. Міжнародна

науково-практична конференція «Новини науки: дослідження, наукові відкриття, високі технології» - ΛΌГОΣ, Україна, Харків, 31.03.2019, 2 с.

64. Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Оцінювання стійкості гетерогенних мереж з використанням методів теорії перколяції. “Сучасні наукові інновації” (частина II): матеріали III Міжнародній науково-практичній конференції м. Київ, 16-17 лютого 2019 року, 2 с.

65. Шапран О.О., Гогонянц С.Ю., Прокопенко А.А. Вимоги до процесу функціонування системи дистанційного навчання вищого військового закладу освіти. Scientific discussion (Praha, Czech Republic). vol 1, No 52, 2021, 31-34 с.

66. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Махно Є.П. Модель інтелектуалізації планування часу на виконання навчального завдання у системі дистанційного навчання. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (40), 2021, с. 143-152.

67. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Судніков Є.О., Твардовський В.Г. Методика розробки web-додатку на основі порталу LIFERAY. Сучасні інформаційні технології у сфері безпеки та оборони. № 2 (38), 2020, с.71-80.

68. Шапран О.О., Махно Є.П. Особливості вибору системи управління дистанційною навчальною діяльністю. 4-та міжнародна науково-практична конференція “Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)”, НУОУ імені Івана Черняховського, м. Київ, 2021 р., с.64-65.

69. Шапран О.О., Салкуцан С.М., Тищенко М.Г. Дистанційне навчання у Збройних Силах України. 3-а міжнародна науково-практична конференція “Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів

закладів вищої освіти)”, матеріали доповідей, НУОУ імені Івана Черняховського, м. Київ, 2020 р., с. 91-96.

70. Шапран О.О., Сергієнко В.Д., Павлунько М.Я., Мулявка А.С. Особливості впливу акустичної зброї на особовий склад військових формувань в умовах ведення не конвенційних воєнних дій. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (37), 2020, с.93-96.

71. Шапран О.О., Тарасенко Н.М., Судніков Є.О., Прокопенко А.А. Впровадження цифрової бібліотеки в освітньо-наукову діяльність. Науково-технічна конференція молодих вчених “Актуальні проблеми інформаційних технологій”, КНУ ім. Т.Шевченка, 19-20 жовтня 2022 року, с. 35-36.

72. Шапран О.О., Тищенко М.Г., Гогонянц С.Ю. Прогноз значень показників можливостей системи навчання на найближчу перспективу. Збірник доповідей 2-ої міжнародної науково-практичної конференції “Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)”, НУОУ імені Івана Черняховського, м. Київ, 2019 р., 3 с.

73. Шапран О.О., Тищенко М.Г., Гогонянц С.Ю., Особливості алгоритмізації процедур комп’ютерного адаптивного тестування. Збірник матеріалів Всеукраїнської науково-методичної конференції «Забезпечення якості вищої освіти» 08 - 10 квітня 2020 р., Одеська національна академія харчових технологій, 2 с.

74. Шапран О.О., Тищенко М.Г., Махно Є.П. Захист даних в інтерактивному освітньому середовищі. Проблеми моделювання та розроблення інформаційних систем: матеріали VI науково-практичної інтернет-конференції (Дрогобич, 4 квітня 2022 року). – Дрогобич : ДДПУ ім. І. Франка, 2022. – 98 с.

75. Шапран О.О., Тищенко М.Г., Прокопенко А.А. Функції дистанційного навчання у системі підготовки військових фахівців. Збірник XXVIII Міжнародної науково-практичної конференції: “Інформаційні

технології: наука, техніка, технологія, освіта, здоров'я. Micro CAD-2020", 14 травня 2020 року (м. Харків) Військовий інститут танкових військ НТУ "ХПІ".

76. Штовба С.Д., Галущак А.В. Ідентифікація багатофакторних залежностей за допомогою баз знань. – Вінниця : ВНТУ, 2015. – 96 с.

77. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління. – К.: 2022. – 307 с.

78. Abhilash Chakraborty, Anupam Biswas, Ajoy Kumar Khan. Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. https://doi.org/10.48550/arXiv.2209.13454

79. Air Defense Planning from an Impact of a Group of Unmanned Aerial Vehicles based on Multi-Agent Modeling / Pavlo Shchypanskyi, Vitalii Savchenko, Oleksii Martyniuk, Ihor Kostiuk // International Journal of Emerging Trends in Engineering Research. Volume 8. No. 4, April 2020. 1302-1308.

80. Al-Yaseen, W., Othman, Z., Ahmad Nazri, M.Z.: Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. Expert Systems with Applications: An International Journal. Volume 67, Issue C, January 2017, pp. 296–303. https://doi.org/10.1016/j.eswa.2016.09.041

81. Analysis and design of a hybrid load management method for the IoT networks / V.Savchenko, V.Druzhynin, M.Tverdohlib, Y.Ivanichenko, N. Dovzhenko, Z. Brzhevska, V. Chorna // International Journal of Advanced Trends in Computer Science and Engineering. Volume 9, No.1, January – February 2020. pp. 552 – 557.

82. Analysis of Social Network Parameters and the Likelihood of its Construction / V. Savchenko, V. Akhramovych, A. Tushych, I. Sribna, I. Vlasov // International Journal of Emerging Trends in Engineering Research. Volume 8 No. 2 (February 2020). pp. 271 – 276.

83. Aurélien Géron Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition, 2019. – 510 p.

84. Baptista I., Shiaeles S. and Kolokotronis N. A Novel Malware Detection System Based on Machine Learning and Binary Visualization, 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8757060.

85. Barbara, D., Couto, J., Jajodia, S., Popyack, L., Wu, N.: Adam: Detecting intru- sions by data mining pp. 5–6 (07 2001)

86. Bose, S., Barao, T., Liu, X.: Explaining ai for malware detection: Analysis of mechanisms of malconv. In: 2020 International Joint Conference on Neural Networks (IJCNN). pp. 1–8 (2020)

87. Buchyk S., Toliupa S., Symonychenko Y., Symonychenko A., Platonenko A. Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 117 –124. URL: http://ceur-ws.org/Vol-2923/paper13.pdf. (дата звернення: 10.05.2023).

88. Charu C. Aggarwal Neural Networks and DeepLearning, Springer International Publishing AG, part of Springer Nature 2018. – 752p.

89. Chowdhury, M., Rahman, A., Islam, M.R.: Malware analysis and detection using data mining and machine learning classification. pp. 266–274 (01 2018). https://doi.org/10.1007/978-3-319-67071-3 33 (дата звернення: 10.05.2023).

90. Coull, S., Gardner, C.: Activation analysis of a byte-based deep neural network for malware classification. pp. 21–27 (05 2019). https://doi.org/10.1109/SPW.2019.00017 (дата звернення: 10.05.2023).

91. Dakhno, N., Kravchenko, Y., Lunin, L., Pliushch, O.,Trush, O., Shevchenko, H. Analysis of VANET Connection Quality in Dynamic

Environment. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 255–258.

92. Detection of Slow DDoS Attacks based on Time Delay Forecasting / Vitalii Savchenko, Valeriia Savchenko, Oleksandr Laptiev, Oleksander Matsko, Ivan Havryliuk, Kseniia Yerhidzei and Iryna Novikova // Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum “DIGITAL REALITY”, September 13 − 19, 2021, Odesa, Ukraine.

93. Detection of Slow DDoS Attacks based on User’s Behavior Forecasting / Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova // International Journal of Emerging Trends in Engineering Research. Volume 8. No. 5, May 2020. 2019-2025.

94. Fractal functions and their application to source data coding / Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, February 2022. pp.424-435.

95. Francois Chollet Deep Learning with Python, Second Edition - Manning Publications, 2021. – 386 p.

96. Hashemi, H., Azmoodeh, A., Hamzeh, A., Hashemi, S.: Graph embedding as a new approach for unknown malware detection. Journal of Computer Virology and Hacking Techniques 13 (08 2017). https://doi.org/10.1007/s11416-016-0278-y

97. Haykin, Simon Neural networks and learning machines. Pearson Education Ltd. 3rd ed. , 2008. – 904p.

98. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement / Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov // In Proceedings of the IEEE International Conference on Advanced Trends in Information Theory, ATIT`2020, Kyiv: IEEE Ukraine Section, 2020, pp.

99. M. J. Hossain Faruk et al., "Malware Detection and Prevention using Artificial Intelligence Techniques," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 5369-5377, doi: 10.1109/BigData52589.2021.9671434.

100. ISO IEC 27005-2018 Інформаційні Технології – Методи безпеки — Стандарт управління ризиками інформаційної безпеки.

101. ISO/IEC 27001:2018. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2018.

102. ISO/IEC 27002:2019. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

103. ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою.

104. ISO/IEC 27007:2020. Інформаційна безпека, кібербезпека та захист конфіденційності – Рекомендації щодо аудиту систем управління інформаційною безпекою.

105. ISO/IEC 27032 – Рекомендації щодо кібербезпеки.

106. ISO/IEC 27035-1:2016. Інформаційні технології. Методи безпеки. Управління інцидентами інформаційної безпеки. Частина 1. Принципи управління інцидентами

107. ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 2. Посібник з планування та підготовки до реагування на інциденти.

108. ISO/IEC 27035-3:2020. Інформаційна технологія. Управління інцидентами інформаційної безпеки. Частина 3. Настанови щодо операцій реагування на інциденти ІКТ.

109. Johns, J.: Representation learning for malware classification. https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/malware-

classification-slides.pdf (2017), [Online; accessed 19-May-2022] (дата звернення: 10.05.2023).

110. Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., Roli, F.: Adversarial malware binaries: Evading deep learning for malware detection in executables. 2018. https://doi.org/10.48550/ARXIV.1803.04173 (дата звернення: 10.05.2023).

111. Kosko B. Fuzzy Systems as Universal Approximators. IEEE Trans. on Computers. –Vol. 43, No 11, 1994, pp. 1329-1333.

112. Kravchenko Y., O. Afanasyeva, M. Tyshchenko,S. Mykus, “Intellectualisation of Decision Support Systems For Computer Networks: Production-Logical F-Inference”, International conference Information Technology and Interactions, IT&I-2020, CEUR Workshop Proceedings, 2021, 2845, pp. 117–126.

113. Kravchenko Y., O. Leshchenko, N. Dakhno,V. Deinega, H. Shevchenko, O. Trush, “Intellectual fuzzy system air pollution control”, IEEE 2nd International Conference on Advanced Trends in Information Theory, ATIT`2020, Proceedings, pp. 186–191.

114. Kravchenko, Y., Dakhno, N., Leshchenko, O., Tolstokorova, A. “Machine learning algorithms for predicting the results of COVID-19 coronavirus infection”, International conference Information Technology and Interactions, IT&I-2020, CEUR Workshop Proceedings, 2021, 2845, pp. 371–381.

115. Kravchenko, Y., Leshchenko, O., Dakhno, N., Pliushch, O.,Trush, O., Yermakov, Y. Development of Model of Artificial Ecosystem on the Basis of Genetic Algorithm. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 199–203.

116. Kreuk, F., Barak, A., Aviv-Reuven, S., Baruch, M., Pinkas, B., Keshet, J.: Deceiv-ing end-to-end deep learning malware detectors using adversarial examples. No 10, 2019, pp. 1-8. https://doi.org/10.48550/arXiv.1802.04528 (дата звернення: 10.05.2023).

117. Luo, B., Xia, J.: A novel intrusion detection system based on feature generation with visualization strategy. Expert Systems with Applications 41, 41394147 (07 2014). (дата звернення: 10.05.2023).

118. Mahajan, R., Siddavatam, I.: Phishing website detection using machine learning algorithms. International Journal of Computer Applications, 2018, no 23, vol 181, pp.45-47.

119. Mamdani E.H., Assilian S. An Experiment in Linguistic Synthesis with Fuzzy Logic Controller. Int. J. Man-Machine Studies. Vol. 7, No 1, 1975, pp.1-13.

120. Mark Fenner Machine Learning with Python for Everyone - Addison-Wesley Professional; 1st edition (August 16, 2019). – 592p.

121. Mashkov O. A. , Murasov R. K. , Kravchenko Y. V. , Dakhno N. B. , Leschenko O. A., Trush O. V. Optimal forecast algorithm based on compatible linear filtration and extrapolation. Mathematical Modeling And Computing, 2021, 8(2), pp. 157–167. DOI: https://doi.org/10.23939/mmc2021.02.157 (дата звернення: 10.05.2023).

122. McLaughlin, N., Doup´e, A., Ahn, G., Martinez-del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., Safaei, Y., Trickel, E., Zhao, Z.: Deep android malware detection. 2017, no 3, pp. 301–308. https://doi.org/10.1145/3029806.3029823 (дата звернення: 10.05.2023).

123. Method of detecting random signals based on determining the deviations of the main parameters of radio signals / Oleksandr Laptiev, Vitalii Savchenko, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma // International Journal of Advanced Trends in Computer Science and Engineering. Volume 9, No.5, September - October 2020. 9204-9209.

124. Method of Determining Trust and Protection of Personal Data in Social Networks / Laptiev O.1, Savchenko V.1, Kotenko A.1, Akhramovych V.1, Samosyuk V. 1, Shuklin G1, Biehun A.2 // International Journal of

Communication Networks and Information Security (IJCNIS) Vol. 13, No. 1, 2021. 15–21.

125. Method of Localızatıon of Means of Illegal Obtaınıng of the Informatıon / Savchenko Vitalii, Laptiev Oleksandr, Serhii Yevseiev, Shmatko Oleksandr, Korol Olha, Barabash Oleg,Oleh Stefurak, Vladyslav Khvostenko // Second International Scientific-Practical Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives'2020 (MIMSCS'2020). December 07-08, 2020. Baku, Azerbaijan

126. Michael Nielsen Neural Networks and Deep Learning [el.src] 2019. - [http://neuralnetworksanddeeplearning.com/]. (дата звернення: 10.05.2023).

127. Model of Alternative Navigation System for High-Precision Weapons / Vitalii Savchenko, Volodymyr Tolubko, Liubov Berkman, Anatolii Syrotenko, Pavlo Shchypanskyi, Oleksander Matsko, Vitalii Tiurin and Pavlo Open'ko // Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. May 27, 2020.

128. Model of an Alternative Navigation System for High-Precision Weapons./ Vitalii Savchenko, Volodymyr Tolubko, Liubov Berkman, Anatolii Syrotenko, Pavlo Shchypanskyi, Oleksander Matsko, Vitalii Tiurin and Pavlo Open'ko // Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. First published - May 27, 2020. Journal of Defense Modeling and Simulation, 2022, 19(3), pp. 255–262. https://doi.org/10.1177/1548512920921955. (дата звернення: 10.05.2023).

129. Model of Connectivity in a Mobile MESH Network for a Group of Unmanned Aerial Vehicles / Vitalii Savchenko, Svitlana Lehominova, Taras Dzyuba, Oleksandr Matsko, Ivan Havryliuk, Iryna Novikova // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022.

130. Naeeni, A. F. Advanced Multi-Agent Fuzzy Reinforcement Learning. Master Thesis Computer Engineering, Nr: E3098D / Alireza Ferdowsizadeh Naeeni. – Dalarna University, Sweden, 2004. – 99 p.

131. Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex, « 201 pages, 11 June 2015, PDF, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf . (дата звернення: 10.05.2023).

132. Rokon, M.O.F., Islam, R., Darki, A., Papalexakis, E., Faloutsos, M.: Sourcefinder: Finding malware source-code from publicly available repositories in github. No 10, 2020, pp. 149-163.

133. Savchenko V. Commercial Encryption Protocols for Military Applications / V. Savchenko, S. Dovbeshko, O. Matsko // Сучасний захист інформації. 2018, № 1 (33). С. 11-16.

134. Savchenko V. Composite Radioisotope Coating Parameters and Reflecting Characteristics Calculation Selection Method / Savchenko V., Zaika V., Trembovetskyi M., Shuklin G., Berkman L., Storchak K., Rolin I. // International Journal of Advanced Trends in Computer Science and Engineering. Volume 8, No.5, September - October 2019. – P. 2246-2251. https://doi.org/10.30534/ijatcse/2019/60852019. (дата звернення: 10.05.2023).

135. Savchenko V. Influense of Composit Materials Nonlinear Properties with Radioisotope Inclutions on Reflected Radiations / Savchenko V., Vorobiov O., O. Tkalenko, Polonevych O., Shuklin G., Trembovetskyi M., Zaika V., Konopliannykova M. // International Journal of Advanced Trends in Computer Science and Engineering. 2019. No.6. P. 2716-2720.

136. Savchenko V. Network traffic forecasting based on the canonical expansion of a random process // V.Savchenko, O.Matsko, O.Vorobiov,

Y.Kizyak, L.Kriuchkova, Y.Tikhonov, A.Kotenko // Eastern European Journal of Enterprise Technologies. 2018. vol 3, NO 2 (93) (2018). P. 33-41.

137. Savchenko V. The Method of Hidden Transmitters Detection based on the Differential Transformation Model / Laptiev O., Shuklin G., Savchenko V., Barabash O., Musienko A., Haidur H. // International Journal of Advanced Trends in Computer Science and Engineering. 2019. No 6. pp. 2840-2846.

138. Savchenko V. The Method of Searching for Digital Means of Illegal Obtaining of Information on the Basis of Cluster Analysis // Sachenko V.A., Laptev A.A., Barabash O.V., Sachenko V.V., Matsko A.I. // Magyar Tudományos Journal (Budapest, Hungary). № 31 (2019). pp. 33-37.

139. Savchenko V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi / Laptev A.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. // International Journal of Advanced Research in Science, Engineering and Technology. Vol. 6, Issue 7 , July 2019. pp. 10101-10105.

140. Schultz, M., Eskin, E., Zadok, F., Stolfo, S.: Data mining methods for detection of new malicious executables. No 02, 2001, pp. 38–49.

141. Shapran O. Yudin O., Artemov V., Tyshchenko M., Makhno Y., Tarasenko N., Forecast Model of Technical State of Telecommunication System: Intelligent Statistical Data Processing. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT-2021) Conference Proceedings, pp. 165-168. (Scopus)

142. Shapran O., Gawliczek, P., Krykun, V., Tarasenko, N., Tyshchenko, M., Computer Adaptive language testing according to NATO STANAG 6001 requirements. Advanced Education, Vol. 8(17), 2021, pp. 19-26. (Web of Science)

143. Shapran O., Kyva V., Koshlan O., Krykun V., Zaika L., Sudnikov Y. The Experience of Implementing a Digital Library in the Educational and Research Activities of the National Defence University of Ukraine named after Ivan Cherniakhovskyi. TEM Journal. Vol 11, Issue 3, pp. 1128-1139. (Scopus)

144. Shapran O., Tyshchenko M. Features of the students' self-work organization of higher military educational institutions under the conditions of the interactive educational environment. Journal of Scientific Papers "Social development & Security", vol 6, no 4, 2018, pp. 54-62.

145. Shapran O., Tyshchenko M., Sudnikov Y., Makhno Y., Gawliczek P. Distance learning system of the professional military education institution: problematic issues of formation. Journal „Civitas et Lex", no 1(37), 2023, pp. 17-25.

146. Sharma, S., Challa, R., Sahay, S.: Detection of advanced malware by machine learning techniques. No 03, 2019.

147. Shevchenko, H., Dakhno, N., Leshchenko, O., Barabash, O., Kravchenko, Y., Dudnik, A. Using Mathematical Optimization Methods to Maximize Audience Reach with Budget Constraints.2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 249–254.

148. Shrestha, P., Maharjan, S., Ramirez-de-la Rosa, G., Sprague, A., Solorio, T., Warner, G.: Using string information for malware family identification. No 11, 2014, pp. 686–697. https://doi.org/10.1007/978-3-319-12027-0 55. (дата звернення: 10.05.2023).

149. Sugeno M. Industrial applications of fuzzy control. NorthHolland, Amsterdam, 1985. – 269 p.

150. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O.Laptiev, O.Milov, V. Savchenko and others. – Kharkiv: PC Technology Center, 2021. – 188 p.

151. The method of localization of signals of radio transmitting devices / Vitalii Savchenko, Oleksandr Laptiev, Vitalii Ponomarenko, Taras Dzyuba, Yuriy Shcheblanin and Valeriia Savchenko // Third International Scientific-Practical Conference «Modern Information, Measurement and Control Systems: Problems, Applications and Perspectives 2022 (MIMCS'2022)", 4-5 November, 2022. Antalya, Türkiye.

152. The Model of Localization Precision for Detection of Hidden Transmitters / Savchenko Vitalii, Syrotenko Anatolii, Shchypanskyi Pavlo, Matsko Oleksander, Laptiev Oleksander // International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-9 Issue-4, February 2020, ISSN: 2278-3075 (Online). pp. 2114-2119.

153. The Model of Secure Social Networks Activity Based on Graph Theory / P. Shchypanskyi, V. Savchenko, V. Akhramovych, T. Muzshanova, S. Lehominova, V. Chegrenets // International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-9 Issue-4, February 2020, ISSN: 2278-3075 (Online). P 1803-1810.

154. Toliupa S., Parkhomenko I., Shvedova H. Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 463–468). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AICT.2019.8847746. (дата звернення: 10.05.2023).

155. Wang Y., Ying L., Hua Z.On the extent analysis method for fuzzy AHP and its applications. European Journal of Operational Research, – Vol. 186, 2008, pp. 735–747.

156. Ye, Y., Chen, L., Hou, S., Hardy, W., Li, X.: Deepam: a heterogeneous deep learning framework for intelligent malware detection. Knowledge and Information Systems 54, pp. 1–21 (02 2018). https://doi.org/10.1007/s10115-017-1058-9 . (дата звернення: 10.05.2023).

157. Zadeh L. A. Fuzzy sets. Journal of Information and control, No 8, 1965, pp. 338-353.

158. Zhu, H.J., You, Z.H., Zhu, Z., Shi, W.L., Cheng, L.: Droiddet: effective and robust detection of android malware using static analysis along with rotation forest model. Neurocomputing. Volume 272, 10 January 2018, pp. 638-

646. https://doi.org/10.1016/j.neucom.2017.07.030/ (дата звернення: 10.05.2023).

159. Jang J.-S. R. ANFIS: Adaptive-Network-based Fuzzy Inference System. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 1993. Vol. 23. no. 3. pp. 665−685.

ДОДАТКИ

Додаток А

Акт впровадження

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки заступника начальника університету з навчальної роботи
полковник
Микола ПАЛАМАР
"26" 09 2023 року

АКТ №609/10/268

впровадження в освітній процес Національного університету оборони України наукових результатів дисертаційного дослідження начальника науково-дослідного відділу перспектив розвитку електронних засобів навчання наукового центру дистанційного навчання полковника **ШАПРАНА Олександра Олександровича** на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології на тему: "Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України"

Підстава: наказ начальника Національного університету оборони України імені Івана Черняховського від 15 липня 2022 року № 213 "Про організацію оцінки впровадження наукових результатів дисертацій в освітній процес та наукову і науково-технічну діяльність університету".

Комісія у складі:

голови – начальника наукового центру дистанційного навчання Національного університету оборони України, кандидата технічних наук, старшого дослідника, полковника ТИЩЕНКА М.Г.;

членів комісії:

заступника начальника науково-методичного центру організації наукової та науково-технічної діяльності Національного університету оборони України, кандидата військових наук, старшого дослідника, полковника КУРБАНА В.А.;

заступника начальника науково-методичного центру організації освітньої діяльності Національного університету оборони України, кандидата педагогічних наук, полковника ТОРЧЕВСЬКОГО Р.В.;

старшого наукового співробітника науково-дослідного відділу перспектив розвитку електронних засобів навчання наукового центру дистанційного навчання Національного університету оборони України, підполковника СУДНІКОВА Є.О.

розглянула надані матеріали в межах дисертаційного дослідження Шапрана Олександра Олександровича, які впроваджені в результати науково-дослідної роботи шифр "Технології-ДН", (державний обліковий номер: 0223U003920),

Акт впровадження

(інв. № 12371), (робота відпрацьована у науковому центрі дистанційного навчання Національного університету оборони України).

Комісія встановила:

1. Результати дисертаційного дослідження полковника ШАПРАНА Олександра Олександровича реалізовані у науково-дослідній роботі шифр "Технології-ДН":

у розділі 1 "Аналіз існуючих підходів щодо цифровізації та інтелектуалізації системи дистанційного навчання Збройних Сил України";

у пункті 1.1 "Об'єктивні передумови розвитку цифровізації в Збройних Силах України";

у розділі 2 "Обгрунтування вимог до цифровізації та інтелектуалізації системи дистанційного навчання у Збройних Силах України";

у пункті 2.1 "Аналіз процесів цифровізації системи дистанційного навчання у Збройних Силах України";

у пункті 2.3 "Вимоги до цифровізації системи дистанційного навчання у Збройних Силах України";

у розділі 5 "Розроблення методичних рекомендацій щодо реалізації онлайн-курсу "Розвитку цифрових компетентностей користувачів системи дистанційного навчання у Збройних Силах України"";

у пункті 5.1 "Рекомендації щодо реалізації онлайн-курсу "Розвитку цифрових компетентностей користувачів системи дистанційного навчання у Збройних Силах України"".

2. Результати дисертаційного дослідження вважати реалізованими в освітньому процесі Національного університету оборони України. Реалізацією отриманих результатів є розроблені методичні рекомендації щодо реалізації онлайн-курсу розвитку цифрової компетентності користувачів системи дистанційного навчання Збройних Сил України та окремі навчальні питання методичної розробки "Курсу підвищення кваліфікації наукових і науково-педагогічних працівників вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти з питань організації та використання технологій дистанційного навчання в Збройних Силах України".

Голова комісії:

полковник Максим ТИЩЕНКО

Члени комісії:

полковник Володимир КУРБАН

полковник Руслан ТОРЧЕВСЬКИЙ

підполковник Євген СУДНІКОВ

Акт впровадження

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки заступника начальника університету з навчальної роботи
полковник
Микола ПАЛАМАР
"26" 09 2023 року

АКТ № 609/10/269
впровадження в освітній процес Національного університету оборони України наукових результатів дисертаційного дослідження начальника науково-дослідного відділу перспектив розвитку електронних засобів навчання наукового центру дистанційного навчання полковника ШАПРАНА Олександра Олександровича на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології на тему: "Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України"

Підстава: наказ начальника Національного університету оборони України імені Івана Черняховського від 15 липня 2022 року № 213 "Про організацію оцінки впровадження наукових результатів дисертацій в освітній процес та наукову і науково-технічну діяльність університету".

Комісія у складі:

голови – начальника наукового центру дистанційного навчання Національного університету оборони України, кандидата технічних наук, старшого дослідника, полковника ТИЩЕНКА М.Г.;

членів комісії:

заступника начальника науково-методичного центру організації наукової та науково-технічної діяльності Національного університету оборони України, кандидата військових наук, старшого дослідника, полковника КУРБАНА В.А.;

заступника начальника науково-методичного центру організації освітньої діяльності Національного університету оборони України, кандидата педагогічних наук, полковника ТОРЧЕВСЬКОГО Р.В.;

старшого наукового співробітника науково-дослідного відділу перспектив розвитку електронних засобів навчання наукового центру дистанційного навчання Національного університету оборони України, підполковника СУДНІКОВА Є.О.

розглянула надані матеріали в межах дисертаційного дослідження Шапрана Олександра Олександровича, які впроваджені в результати науково-дослідної

Акт впровадження

роботи шифр "Система-ДН" (державний обліковий номер: 0221U105577), (інв. № 9985) (робота відпрацьована у науковому центрі дистанційного навчання Національного університету оборони України):

Комісія встановила:

1. Результати дисертаційного дослідження полковника ШАПРАНА Олександра Олександровича реалізовані у науково-дослідній роботі:

у розділі 1 "Аналіз можливих варіантів побудови системи дистанційного навчання вищого військового навчального закладу з урахуванням досвіду збройних сил провідних країн світу";

у пункті 1.3 "Формування можливих варіантів побудови системи дистанційного навчання вищого військового навчального закладу";

у розділі 4 "Розроблення типової системи дистанційного навчання вищого військового навчального закладу";

у пункті 4.1 "Аналіз результатів розрахунку показників якості функціонування системи дистанційного навчання вищого військового навчального закладу";

у розділі 5 "Розроблення рекомендацій щодо організації роботи системи дистанційного навчання вищого військового навчального закладу";

у пункті 5.2 "Рекомендації щодо вибору комплексу спеціального програмного забезпечення системи дистанційного навчання вищого військового навчального закладу";

у пункті 5.3 "Рекомендації щодо організації роботи системи дистанційного навчання вищого військового навчального закладу".

2. Результати дисертаційного дослідження вважати реалізованими в освітньому процесі Національного університету оборони України. Реалізацією отриманих результатів є методичні рекомендації щодо підвищення ефективності функціонування системи дистанційного навчання в Збройних Силах України.

Голова комісії:

полковник Максим ТИЩЕНКО

Члени комісії:

полковник Володимир КУРБАН

полковник Руслан ТОРЧЕВСЬКИЙ

підполковник Євген СУДНІКОВ

Додаток Б
Список публікацій здобувача

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Shapran O., Tyshchenko M. Features of the students' self-work organization of higher military educational institutions under the conditions of the interactive educational environment. Journal of Scientific Papers "Social development & Security", vol 6 no 4, 2018, pp. 54-62.

2. Шапран О.О., Гогонянц С.Ю., Грицай П.М. Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (34), 2019, с.29-36.

3. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Судніков Є.О., Твардовський В.Г. Методика розробки web-додатку на основі порталу Liferay. Сучасні інформаційні технології у сфері безпеки та оборони. № 2 (38), 2020, с.71-80.

4. Шапран О.О., Гогонянц С.Ю., Прокопенко А.А. Вимоги до процесу функціонування системи дистанційного навчання вищого військового закладу освіти. Scientific discussion (Praha, Czech Republic). Vol 1, No 52, 2021, 31-34 с.

5. Шапран О.О., Кравченко Ю.В., Тищенко М.Г., Махно Є.П. Модель інтелектуалізації планування часу на виконання навчального завдання у системі дистанційного навчання. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (40), 2021, с. 143-152.

6. Shapran O., Gawliczek, P., Krykun, V., Tarasenko, N., Tyshchenko, M. Computer Adaptive language testing according to NATO Stanag 6001 requirements. Advanced Education, Vol. 8(17), 2021, pp. 19-26. (Web of Science)

7. Шапран О., Кравченко Ю., Махно Є., Тищенко М. Модель інтелектуалізації оптимальної траєкторії проходження дистанційного курсу. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (43), 2022, с.105 – 114.

8. Shapran O., Kyva V., Koshlan O., Krykun V., Zaika L., Sudnikov Y. The Experience of Implementing a Digital Library in the Educational and Research Activities of the National Defence University of Ukraine named after Ivan Cherniakhovskyi. TEM Journal. 2022, Vol 11, Issue 3, pp. 1128-1139. (Scopus)

9. Shapran O., Tyshchenko M., Sudnikov Y., Makhno Y., Gawliczek P. Distance learning system of the professional military education institution: problematic issues of formation. Journal „Civitas et Lex”, no 1(37), 2023, pp. 17-25.

10.Шапран О., Махно Є. Аналіз процесів інтелектуалізації системи дистанційного навчання у Збройних силах України. Сучасні інформаційні технології у сфері безпеки та оборони. № 1 (46), 2023, с. 107-114.

11.Шапран О. Моделі підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Телекомунікаційні та інформаційні технології. № 2 (45), 2023, с. 33-45.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12.Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Оцінювання стійкості гетерогенних мереж з використанням методів теорії перколяції: III Міжнародна науково-практична конференція «Сучасні наукові інновації» (частина II), м. Київ, 16-17 лютого 2019 р., 2 с.

13.Шапран О.О., Гогонянц С.Ю., Мельник Я.В. Обґрунтування напрямку дослідження стійкості гетерогенних мереж до кібератак. Міжнародна науково-практична конференція «Новини науки: дослідження, наукові відкриття, високі технології» - ΛΌГОΣ, Україна, Харків, 31 березня 2019 р., 2 с.

14.Шапран О.О., Тищенко М.Г., Гогонянц С.Ю. Прогноз значень показників можливостей системи навчання на найближчу перспективу. 2-а міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2019 р., 3 с.

15.Шапран О.О., Тищенко М.Г., Гогонянц С.Ю. Особливості алгоритмізації процедур комп'ютерного адаптивного тестування. Всеукраїнська науково-методична конференції «Забезпечення якості вищої освіти», 08 – 10 квітня 2020 р., Одеська національна академія харчових технологій, 2 с.

16.Шапран О.О., Тищенко М.Г., Прокопенко А.А. Функції дистанційного навчання у системі підготовки військових фахівців. XXVIII Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. Micro CAD-2020», 14 травня 2020 р., м. Харків, Військовий інститут танкових військ НТУ "ХПІ".

17.Шапран О.О., Гогонянц С.Ю., Клочко А.О. Технології дистанційного навчання у системі військової освіти. XXIII Міжнародна науково-практична конференція "Theoretical and Practical Foundations of Social Process Management", 29-30 червня 2020 р., Сан-Франциско, США, 4 с.

18.Шапран О.О., Салкуцан С.М., Тищенко М.Г. Дистанційне навчання у Збройних Силах України. 3-а міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2020 р., с. 91-96.

19.Шапран О.О., Махно Є.П. Особливості вибору системи управління дистанційною навчальною діяльністю. 4-та міжнародна науково-практична конференція «Проблеми впровадження дистанційного навчання в освітній процес вищих військових навчальних закладів (військових підрозділів

закладів вищої освіти)», НУОУ імені Івана Черняховського, м. Київ, 2021 р., с.64-65.

20.Shapran O. Yudin O., Artemov V., Tyshchenko M., Makhno Y., Tarasenko N., Forecast Model of Technical State of Telecommunication System: Intelligent Statistical Data Processing. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT-2021) Conference Proceedings, pp. 165-168. (Scopus)

21.Шапран О.О., Тищенко М.Г., Махно Є.П. Захист даних в інтерактивному освітньому середовищі. VI науково-практична інтернет-конференція «Проблеми моделювання та розроблення інформаційних систем» 4 квітня 2022 р., м. Дрогобич, ДДПУ ім. І. Франка, – 98 с.

22.Шапран О., Судніков Є., Тарасенко Н. Захист персональних даних методом знеособлення. III науково-практичний вебінар «Забезпечення кібероборони держави» 29 вересня 2022 року м. Київ, НУОУ, 2022. – 192 с.

23.Шапран О.О., Тарасенко Н.М., Судніков Є.О., Прокопенко А.А. Впровадження цифрової бібліотеки в освітньо-наукову діяльність. Науково-технічна конференція молодих вчених “Актуальні проблеми інформаційних технологій”, КНУ ім. Т.Шевченка, 19-20 жовтня 2022 року, с. 35-36.