DOI:**10.33099/2311-7249/2023-48-3-5-10**

УДК: 519.682

Ільїн Дмитро Володимирович
Шовкошитний Ігор Іванович ***(кандидат військових наук, старший науковий співробітник)***

Національний університет оборони України, Київ, Україна

ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ АВТОКОМПЕНСАЦІЙНОГО ПРИНЦИПУ АДРЕСНО-ЧАСОВОЇ СЕЛЕКЦІЇ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКА

Стрімкий розвиток інформаційних технологій призвів до появи нових загроз у сфері кібербезпеки, що вимагає удосконалення існуючих і розроблення нових підходів у сфері захисту інформаційно-телекомунікаційних систем від кіберзагроз. Питанням кіберзахисту мережевих систем, у тому числі військових, присвячено значну кількість досліджень, у яких увага авторів зосереджується переважно на питаннях виявлення кіберзагроз. Водночас, проблеми нейтралізації таких загроз в інформаційно-телекомунікаційних системах, досліджені недостатньо. З урахуванням зазначеного у даній статті висвітлено новий підхід до захисту інформаційно-телекомунікаційних систем на основі автокомпенсаційного принципу адресно-часової селекції (відбору) аномалій шкідливого трафіку. Проведено аналіз підходів до селекції цілей на фоні радіозавад, що використовуються в радіолокації, зокрема, принципів дії автокомпенсатора активних шумових радіозавад і черезперіодного автокомпенсатора пасивних радіозавад, у яких для виділення корисного сигналу на фоні відповідно використовуються розбіжності в напрямках надходження сигналів або розбіжності у часі їх надходження. Зазначені підходи визначені як прототип технічного рішення, що може бути адаптоване для вирішення задачі виділення аномалій мережевого трафіку в інформаційно-телекомунікаційних системах. З урахуванням визначених прототипів запропоновано для захисту інформаційно-телекомунікаційних систем від потенційних кіберзагроз використовувати автокомпенсаційний принцип «адресно-часової селекції» для виділення та нейтралізації аномалій мережевого трафіку. Сутність його полягає у використанні розбіжностей часу і адрес надходження на легальні та на хибні елементи інформаційно-телекомунікаційних систем відповідного синхронізованого очікуваного трафіку й асинхронного аномального (шкідливого) трафіку, який виокремлюється в хибних елементах системи (за допомогою нейромережевого ідентифікатора шкідливих вторгнень) та надається на інші елементи інформаційно-телекомунікаційної системи у вигляді керуючого компенсаційного трафіку для компенсації виявлених у мережі аномалій. Під час написання статті (проведення дослідження) використано методи аналізу та аналогій для визначення прототипів автокомпенсаторів і вибору принципів нейтралізації шкідливих вторгнень. Теоретична значущість отриманих результатів полягає у тому, що запропонований підхід дає змогу удосконалити технології виявлення та нейтралізації аномалій мережевого трафіку в інформаційно-телекомунікаційних системах військового призначення. З практичної точки зору, підхід може бути впроваджений у системах захисту зазначених систем, що значно підвищить їх стійкість до кіберзагроз.

Ключові слова: *інформаційно-телекомунікаційна система, кіберзахищеність, кібербезпека, аномалії мережевого трафіку, автокомпенсатор, адресно-часова селекція.*

Вступ

Постановка проблеми. В умовах стрімкого зростання кіберризиків і кіберзагроз важливим є питання забезпечення кіберзахисту інформаційно-телекомунікаційних систем (далі – ІТС) від шкідливих кібервпливів. Практичний досвід (як вітчизняний, так і світовий) свідчить про те, що перманентний розвиток загальнодоступних технологій та засобів кібервпливу створює небезпеку для існуючих ІТС. У той же час визнається, не зважаючи на суттєву увагу, що приділяється в усіх сферах питанням кібербезпеки, нині практично відсутні ефективні засоби, які б гарантовано захищали ІТС від кіберзагроз. В цих умовах виникає потреба у пошуку нових підходів щодо захисту ІТС (зокрема, ІТС військового призначення). Одним з шляхів при цьому може бути використання у сфері інформаційно-телекомунікаційних технологій принципів і технічних рішень, які використовуються в інших галузях науки і техніки.

Аналіз останніх досліджень і публікацій. Питанням кіберзахисту ІТС, у тому числі систем військового призначення, присвячена значна кількість досліджень та наукових публікацій. Зокрема у [1] запропоновано математичну модель системи виявлення вторгнення з використанням нейронної мережі на основі автоенкодерів, яка формалізує процес виявлення вторгнень у інформаційно-телекомунікаційних мережах військового призначення шляхом становлення взаємозалежностей між базовими атрибутами мережевого трафіку. Увага авторів зосереджена на алгоритмах підвищення точності виявлення вторгнень і проблемах навчання нейромережевої моделі за допомогою машинного навчання.

У роботах [2–5] розглядаються сучасні системи виявлення вторгнень та боротьби з кіберінцидентами, а саме:

системи виявлення кібератак (Intrusion Detection System, IDS) [2];

системи попередження кібератак (Intrusion Prevention System, IPS);

системи виявлення та попередження кібератак (Intrusion Detection and Prevention System, IDPS) [3; 4].

Сучасні IDS/IPS/IDPS функціонують за принципом «глибокого аналізу пакетів даних» («Deep Packet Inspection», DPI) [4; 5], внаслідок чого виконуються у вигляді «надбудови» над оперативно-розшуковими DPI-системами «законного перехоплення» («lawful interception») інтернет-трафіка або у вигляді спеціалізованих вузькопрофільних DPI-систем [4]. Від оперативно-розшукових DPI-систем IDS/IPS/IDPS відрізняються призначенням для пошуку за сигнатурами та блокування в інтернет-трафіку шкідливого програмного забезпечення, а не відбору приватного інтернет/мережевого контенту.

Загалом можна стверджувати, що більшість праць, присвячено проблемам виявлення кіберзагроз, використовують стандартні протоколи, які не завжди є ефективними у випадку комбінованих кібератак на ІТС. Крім того, з точки зору кібербезпеки важливими є також проблеми нейтралізації таких загроз в ІТС. Враховуючи вищезазначене обрана тема статті є актуальною.

Метою статті є висвітлення підходу до захисту інформаційно-телекомунікаційних систем на основі автокомпенсаційного принципу адресно-часової селекції аномалій шкідливого трафіку.

Виклад основного матеріалу дослідження

Для захисту ІТС від шкідливих кібервпливів пропонується використати принцип роботи автокомпенсатора, під яким у загальному плані розуміють пристрій (систему), який автоматично компенсує певні небажані зміни (помилки, завади) у системі з метою підтримання її стабільності або оптимальної роботи.

Прототипом технічного рішення, в якому реалізується цей принцип, є автокомпенсатори радіозавад, які широко відомі з 60-их років минулого століття та масово використовуються практично в усіх сучасних радіолокаційних системах [2; 6]. Для вибору найбільш доцільного варіанту прототипу технології захисту ІТС на основі автокомпенсаційного принципу розглянемо декілька варіантів застосування автокомпенсаторів у галузі радіолокації.

Наприклад, для захисту радіолокаційних станцій (РЛС) від активних шумових радіозавад зазвичай використовується багатоканальний автокомпенсатор, який містить основний та додаткові канали приймання радіосигналів. Принцип дії такого автокомпенсатора наведено на рис. 1.

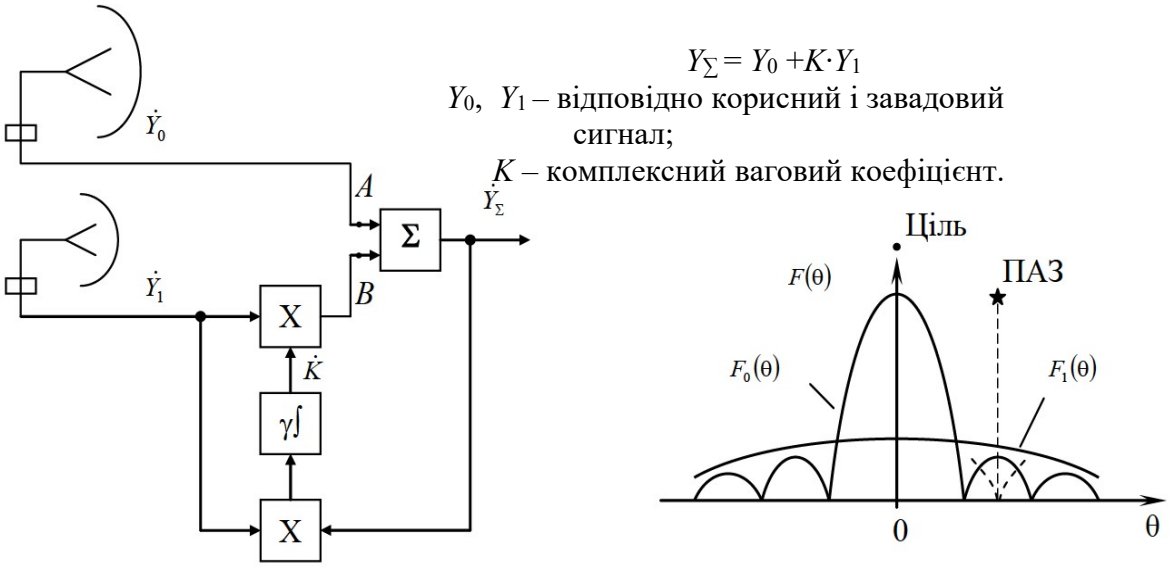

Рисунок 1 – Принцип дії автокомпенсатора активних шумових радіозавад, у якому для виділення сигналу на фоні радіозавад використовуються розбіжності в їхніх напрямках надходження [2]

На основний канал (вхід) автокомпенсатора надходить суміш корисних сигналів та завад, що діють в напрямку основної пелюстки діаграми спрямованості антени (далі – ДСА), а на допоміжні канали прийому – активні шумові завади, що діють по бічних пелюстках ДСА.

Для захисту РЛС від пасивних завад використовуються схеми селекції рухомих цілей та пристрої черезперіодного віднімання. Основним каналом при цьому умовно є поточна суміш радіолокаційних сигналів від цілі, що змінює своє положення з кожним періодом зондування, та пасивної перешкоди, сигнал від якої залишається незмінним. Роль додаткового каналу виконує подібна суміш сигналів, затримана на один період зондування *T*.

Принцип дії такого черезперіодного автокомпенсатора у простішому вигляді наведено на рис. 2.

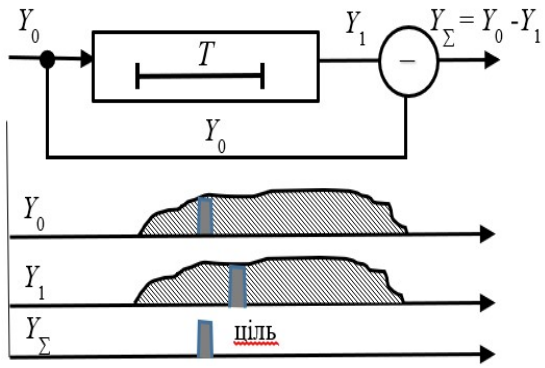

Рисунок 2 – Принцип дії черезперіодного автокомпенсатора

Ці компенсатори досить повно описані у [8] та є елементом когерентних систем селекції рухомих цілей в РЛС і можуть використовувати одну або декількох ліній затримки для підвищення надійності компенсації перешкодових сигналів. Також відомі автокомпенсатори на основі принципу поляризаційної селекції корисних сигналів. Вони частіше застосовуються для компенсації радіолокаційних сигналів, відбитих від метеоутворень (природних пасивних радіозавад).

Можна стверджувати, що більшість традиційних автокомпенсаторів у радіолокаційних системах використовують принцип просторово-часової селекції, який дозволяє виділити корисні сигнали на фоні радіозавад шляхом компенсації сигналів цих завад. Вважаючи це ствердження базовим можна припустити, що подібний принцип за умов певної адаптації може бути реалізований також і у системах захисту ІТС. За аналогію із РЛС, у яких автокомпенсація завад заснована на принципі «просторово-часової селекції», захист ІТС може базуватись на автокомпенсаційному принципі «адресно-часової селекції», який пропонується розглянути нижче.

Розглянемо модель умовної ІТС військового призначення, у якій для виявлення та нейтралізації аномалій мережевого трафіку використана технологія автокомпенсації деструктивного впливу на основі зазначеного принципу (рис. 3). Слід зауважити, що прототипом скоріше є черезперіодний автокомпенсатор пасивних завад (рис. 2), оскільки принцип його дії також базується на чіткій часовій синхронізації роботи каналів компенсації.

Як наведено на рис. 3 модель умовної ІТС містить такі елементи:

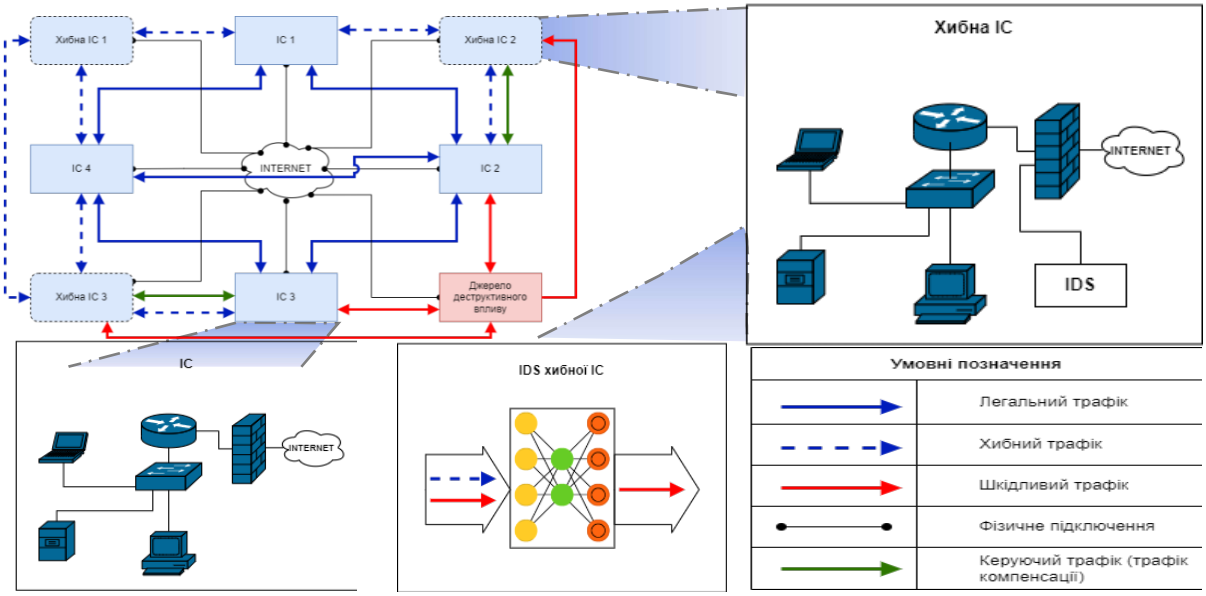

Рисунок 3 – Модель умовної ІТС військового призначення, у якій для виявлення та нейтралізації аномалій мережевого трафіку використана технологія автокомпенсації деструктивного впливу на основі принципу «адресно-часової селекції»

справжні інформаційні системи (ІС) – ІС1, …, ІС4;

хибні інформаційні системи (далі – ХІС) – ХІС1, ХІС2,… (у складі яких IDS – нейромережеві ідентифікатори шкідливих вторгнень);

джерело деструктивного впливу (шкідливого трафіку).

Усі елементи умовної ІТС мають фізичне з'єднання через мережу Internet.

Відмінність справжніх та хибних ІС полягає у наявності у складі останніх додаткового елемента – ідентифікатора шкідливого трафіку на основі нейронної мережі. Слід відмітити, що саме ХІС є ключовим елементом для ідентифікації шкідливого трафіку.

Між елементами ІТС здійснюється легальний та хибний трафік (відповідно S_0 та S_1), який може доповнюватись шкідливим трафіком (S_D) від джерела деструктивного впливу. Припустимо, що:

усі елементи ІТС (справжні та хибні) синхронізовані за часом, тобто усі вхідні та вихідні процеси відбуваються з прив'язкою до єдиної системи часу;

легальний та хибний трафік в ІТС синхронізовані між собою;

хибний трафік додатково синхронізований за структурою та адресою надходження (тобто у ХІС завжди є дані щодо варіантів хибного трафіку та часу його надходження на ту чи іншу ХІС);

шкідливий трафік надходить на елементи ІТС асинхронно.

Зазначені припущення є базовими для принципу «адресно-часової селекції».

Оскільки шкідливий трафік може надходити на входи справжніх та хибних елементів ІТС (ІС та ХІС) змішуючись із легальним трафіком, вхідні сигнали інформаційних та ХІС в загальному випадку можна записати так:

$$S_0' = S_0 + S_D,\ \ S_1' = S_1 + S_D. \qquad (1)$$

У ХІС, у яких відповідно вищезазначених припущень завжди є дані щодо варіантів хибного трафіку та часу його надходження, за допомогою нейромережевих методів розв'язання задач класифікації здійснюється ідентифікація шкідливого деструктивного трафіку:

$$S_D = S_1' - S_1. \qquad (2)$$

Фактично хибні інформаційні системи в ІТС виконують функцію дискримінатора аномалій мережевого трафіку. Подібні пристрої широко застосовуються у технічних електронних пристроях для відбору електричних імпульсів із заданими параметрами або для одержання інформації про відхилення певних параметрів електричних періодичних сигналів від заданої величини [9].

Надалі виявлені параметри шкідливого трафіку заносяться до бази даних, а також з виходу (виходів) хибних інформаційних систем надаються на інші елементи ІТС, зокрема на справжні ІС у вигляді керуючого трафіку або трафіку компенсації (рис. 3), який міститиме правила фільтрації мережевого трафіку з урахуванням параметрів виявленого шкідливого трафіку. З урахуванням означеного, на справжні ІС надходить суміш легального та шкідливого трафіку (основний канал автокомпенсатора деструктивного впливу), а хибні ІС фактично стають додатковим каналом автокомпенсатора. У результаті у справжніх ІС відбувається узгоджена автоматична компенсація шкідливого трафіка та забезпечення циркуляції в ІТС лише легального трафіка:

$$S_0 = S_0' - (S_1' - S_1). \qquad (3)$$

Автокомпенсаційний принцип виділення та нейтралізації аномалій мережевого трафіка в ІТС наведений на рис. 4.

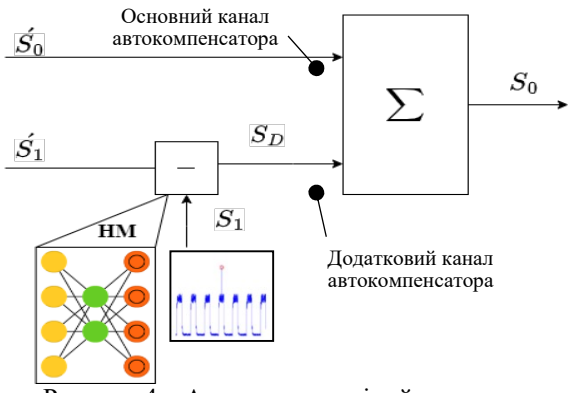

Рисунок 4 – Автокомпенсаційний принцип виділення та нейтралізації аномалій мережевого трафіку в інформаційно-телекомунікаційних системах

Отже, описана послідовність дій реалізує автокомпенсаційний принцип «адресно-часової селекції» аномалій мережевого трафіку, який може бути впроваджений в системах захисту ІТС військового призначення.

Висновки й перспективи подальших досліджень

У статті вдосконалено метод Дейкстри для пошуку найкоротших маршрутів між вузлами зв'язку в системі військового зв'язку завдяки його використанню замість матриці інцидентності вузлів зв'язку у стандартному алгоритмі матриці інцидентності вузлів і ліній зв'язку. Такий підхід більш за все відповідає потребам управління системою військового зв'язку. Він дозволяє найоптимальніше сформувати значення вагових коефіцієнтів ліній зв'язку завдяки визначенню уточнених експлуатаційних витрат для функціонування ліній зв'язку кожним окремим вузлом зв'язку. Визначення вагових коефіцієнтів ліній зв'язку можна реалізувати у вигляді окремої інформаційно-аналітичної задачі або удосконалити алгоритм Дейкстри шляхом введення до нього додаткових блоків. Використання матриці вторинної інцидентності вузлів зв'язку в алгоритмі Дейкстри також дозволить спростити обчислювальну складність алгоритму.

Математичне моделювання на основі спрощеної моделі системи військового зв'язку, що наведена на рисунку 2, підтвердило ефективність удосконаленого методу.

Такий підхід може бути поширений на інші випадки інтерпретації вагових коефіцієнтів в алгоритмі, окрім експлуатаційних витрат. Наприклад, це можуть бути характеристики, що мають ймовірнісний характер. Такі як імовірність доставки інформаційних повідомлень, імовірність бітової помилки, імовірності стійкості ліній і вузлів зв'язку в умовах ведення сучасних інтенсивних бойових дій та інші.

Список бібліографічних посилань

1. Ільїн Д. В., Старинський І. М. Математична модель системи виявлення вторгнень з використанням нейронної мережі на основі автоенкодерів. *Сучасні інформаційні технології у сфері безпеки та оборони* : наук. журн. / Нац. ун-т оборони України. Київ. 2023. № 2 (47). С. 113–118**. 2. Що таке SOC.** URL: https://rvision.pro/2-1-chto-takoesoc-perevod-gajda-mitre (дата звернення: 14.11.2023). **3. Tatsuhiko A. , Yukiko Y., Yutaka T.** Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats. *NEC Technical Journal*. *Special Issue on Cybersecurity*. 2018. Vol. 12. No. 2. pp. 34–37. **4. Scarfone K., Mell P.,** Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, Special Publication 800-94. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, February 2007. **5. Mueller M., Kuehn A.**, Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change. URL: https://www.econinfosec.org (дата звернення: 04.11.2023). archive/weis2013/papers/MuellerKuehnWEIS2013.pdf. **6. Васюта К. С., Тесленко О. В. , Купрій В. М., Малишев О. А.** Основи побудови радіолокаційних засобів розвідки повітряного простору : конспект лекцій. Харків: ХУПС, 2013. 212 с. **7. Адаптивный компенсатор пассивных помех**. URL: https://patents.google.com/patent/RU182620U1/com (дата звернення: 10.10.2023). **8. Справочник по радиолокации** / Под. ред. М. Сколника. Нью-Йорк. 1970. Пер. с англ. (в четырех томах). Том 3. Радиолокационные устройства и системы, 1978. 528 с. **9. Словник з кібернетики** / За ред. академіка В. С. Михалевича. 2-е. вид. Київ, 1989. 751 с.

APPROACH TO PROTECTING INFORMATION AND TELECOMMUNICATION SYSTEMS BASED ON THE AUTO-COMPENSATORY PRINCIPLE OF ADDRESS-TIME SELECTION FOR NETWORK TRAFFIC ANOMALIES

Ilyin Dmytro
Shovkoshytnyi Ihor ***(Candidate of Technical Sciences, Senior Researcher)***

National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *The rapid development of information technologies has led to the emergence of new threats in the field of cyber security, which requires the improvement of existing and the development of new approaches in the field of protection of information and telecommunication systems from cyber threats. The purpose of the article is to highlight the approach to the protection of information and telecommunication systems based on the self-compensating principle of address-time selection of malicious traffic anomalies.*

Research methods. *During the writing of the article (conducting research), the methods of analysis and analogies were used to determine the prototypes of autocompensators and to choose the principles of neutralization of harmful intrusions.*

Analysis of recent researches and publications. *A significant number of studies are devoted to the issue of cyber protection of network systems, including military ones, in which the authors' attention is mainly focused on the issues of identifying cyber threats. At the same time, the problems of neutralizing such threats in information and telecommunication systems have not been sufficiently investigated.*

Presenting the main material. *A new approach to the protection of information and telecommunication systems based on the self-compensating principle of address-time selection (selection) of malicious traffic anomalies is highlighted. An analysis of the approaches used in radar to target selection against the background of radio interference was carried out, in particular, the principles of operation of the autocompensator of active noise radio interference and the periodic autocompensator of passive radio interference, in which differences in the direction of signal arrival or differences in the time of their arrival are used to isolate a useful signal from the background, respectively. The specified approaches are defined as a prototype of a technical solution that can be adapted to solve the problem of identifying network traffic anomalies in information and telecommunication systems. Taking into account the identified prototypes, it is proposed to use the self-compensating principle of "address-time selection" to identify and neutralize network traffic anomalies to protect information and telecommunication systems from potential cyber threats. Its essence consists in the use of time discrepancies and addresses of the arrival of the corresponding synchronized expected traffic and asynchronous anomalous (harmful) traffic to legal and false elements of information and telecommunications*

systems, which is isolated in false system elements (with the help of a neural network identifier of malicious intrusions) and provided to other elements information and telecommunications system in the form of control compensatory traffic to compensate for anomalies detected in the network.

Elements of scientific novelty. *The theoretical significance of the obtained results lies in the fact that the proposed approach makes it possible to improve the technologies for detecting and neutralizing network traffic anomalies in military information and telecommunication systems.*

Practical significance of the article. *From a practical point of view, the proposed approach can be implemented in the protection systems of the specified military information and telecommunication systems, which will significantly increase their resistance to cyber threats.*

Conclusion and the perspectives of future researches. *In the future, it is advisable to develop a detailed mathematical model for compensation of network traffic anomalies in spatially distributed systems based on the proposed principle of "address-time selection" taking into account multiple cyber attacks.*

Keywords: *information and telecommunication system, cyber resilience, cybersecurity, network traffic anomalies, auto-compensator, address-time selection.*

References

1. Ilin, D. V., Starynskyi, I. M., (2023). Mathematical model of an intrusion detection system using a neural network based on auto-encoders. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 2 (47),113–118. **2. What is SOC?** [online]. Available at: https://rvision.pro/2-1-chto-takoesoc-perevod-gajda-mitre [Accessed : 03 September 2023]. **3. Tatsuhiko, A., Yukiko, Y., Yutaka, T.,** (2018). Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats. *NEC Technical Journal. Special Issue on Cybersecurity*. 12, 2, 34-37. **4. Scarfone, K., Mell, P.,** (February 2007). Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, Special Publication 800-94. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930. **5. Mueller, M., Kuehn, A.,** (2013). Einstein on the Breach : Surveillance Technology. Cybersecurity and Organizational Change [online]. Available at: https://www.econinfosec.org/archive/ weis2013/papers/MuellerKuehnWEIS2013.pdf [Accessed : 03 September 2023]. **6. Vasiuta, K. S., Teslenko, O. V., Kuprii, V. M., Malyshev, O. A.,** (2013). Fundamentals of construction of radar airspace reconnaissance equipment : lecture notes. Kharkiv : KhUPS, 212. **7. Adaptive passive interference compensator**. [online]. Available at: https://patents.google.com/patent/ RU182620U1/com [Accessed : 03 September 2023]. **8. Radar Handbook,** (1978). Pod. red. M. Skolnyka. Niu-York. 1970. Per. s anhl. (v chetyrekh tomakh). Tom 3. Radyolokatsyonnye ustroistva y systemy, 528. **9. Dictionary of cybernetics,** (1989). Za red. akademika V. S. Mykhalevycha. 2-e. vyd. Kyiv, 751.