УДК 004.056:621.396.6 DOI: https://doi.org/10.32515/2664-262X.2024.10(41).2.32-38

Д.І. Прокопович-Ткаченко, доц., канд. техн. наук
Університет митної справи та фінансів, м. Дніпро, Україна
В.П. Звєрєв, доц., канд. техн. наук, **В.Г. Бушков,** асп.
Державний торговельно-економічний університет, м. Київ, Україна
Б.С. Хрушков. асп., **О.В. Черкаський**, студ.
Університет митної справи та фінансів, м. Дніпро, Україна

Таргетовані атаки на супутникові інтернет-системи: виклики та підходи до захисту

У статті аналізується одна з наймасштабніших кібератак, спрямована на використання уразливостей супутникового інтернету Starlink, що широко застосовується для забезпечення зв'язку в умовах відсутності традиційної інфраструктури. Зловмисники, використовуючи шкідливе програмне забезпечення, здійснили таргетовані атаки на пристрої, що дозволило їм отримати доступ до конфіденційної інформації та порушити роботу критичних систем. Детально описано методи атак, включаючи впровадження шкідливих програм через PowerShell-дроппери, зміну конфігурацій мережевих пристроїв та збирання чутливих даних. Особливу увагу приділено наслідкам атак, серед яких втрати даних, дестабілізація роботи мережі та уразливість ключової інфраструктури. На основі проведеного аналізу запропоновано рекомендації щодо вдосконалення систем кіберзахисту, зокрема впровадження багаторівневих емерджентно-адаптивних нейромереж, здатних забезпечити моніторинг та реагування у реальному часі. Наголошено на важливості інтеграції міжнародних стандартів інформаційної безпеки, таких як ДСТУ ISO/IEC 27001:2023, для створення ефективної системи захисту, адаптованої до сучасних кіберзагроз.

кібербезпека, супутниковий інтернет, Starlink, шкідливе ПЗ, конфіденційність даних, адаптивні нейромережі, PowerShell-дроппери, таргетовані атаки, уразливості, багаторівневий захист, кіберзагрози

Постановка проблеми. У сучасних умовах цифрової трансформації супутниковий інтернет стає важливим елементом забезпечення стабільного зв'язку в регіонах із відсутністю традиційної інфраструктури або її пошкодженням. Однією з найпоширеніших систем, яка використовується в таких умовах, є Starlink, що забезпечує високу швидкість передачі даних навіть у віддалених районах. Однак, попри значні переваги, супутникові системи зв'язку створюють нові виклики в сфері кібербезпеки. Вразливості цих систем активно експлуатуються зловмисниками, які спрямовують свої зусилля на компрометацію критичної інфраструктури, збирання чутливих даних та дестабілізацію роботи комунікаційних мереж. Останні масштабні кібератаки на супутникові системи демонструють високий рівень організації хакерських угруповань, які використовують сучасні технології, зокрема шкідливе програмне забезпечення, для досягнення своїх цілей. Таргетовані атаки часто включають впровадження PowerShell-дропперів, зміну конфігурацій мережевих пристроїв та збирання даних, що призводить до значних втрат конфіденційної інформації та порушення роботи мереж. Особливу увагу привертає недостатня готовність традиційних систем кіберзахисту до протидії таким загрозам.

Це зумовлює необхідність розробки адаптивних підходів, які враховують динаміку сучасного кіберсередовища. Впровадження багаторівневих систем захисту,

що базуються на емерджентно-адаптивних нейромережах, є перспективним напрямом для забезпечення оперативного моніторингу та швидкого реагування на загрози. Метою даної роботи є аналіз сучасних методів таргетованих атак на супутникові системи зв'язку, оцінка їх впливу на критичну інфраструктуру та розробка рекомендацій щодо вдосконалення кіберзахисту. У роботі також акцентується увага на важливості інтеграції міжнародних стандартів, таких як ДСТУ ISO/IEC 27001:2023, для підвищення стійкості інформаційних систем до нових кіберзагроз.

Аналіз останніх досліджень і публікацій. Атака групи Secret Blizzard на інфраструктуру, що використовує супутниковий інтернет Starlink, підкреслює необхідність впровадження комплексних заходів кібербезпеки. Використання шкідливого програмного забезпечення Amadey та Tavdig свідчить про високий рівень організації та координації зловмисників. Для ефективного захисту інформаційних систем необхідно впроваджувати емерджентно-адаптивні нейромережі, здатні динамічно реагувати на нові загрози та забезпечувати безпеку на всіх рівнях моделі OSI. Це дозволить підвищити конфіденційність, цілісність та доступність даних, особливо в екстремальних польових умовах. Важливим є дотримання національних стандартів, таких як ДСТУ ISO/IEC 27001:2023, що встановлює вимоги до систем управління інформаційною безпекою [1], та ДСТУ ISO/IEC 27002:2023, який надає рекомендації щодо контролю кібербезпеки [2]. Крім того, слід враховувати стандарти НАТО, зокрема STANAG 4586, що визначає вимоги до сумісності систем управління безпілотними літальними апаратами [3]. Дотримання цих стандартів сприятиме підвищенню рівня захисту інформаційних систем та ефективному протистоянню сучасним кіберзагрозам. Застосування методів супутникового моніторингу та геопросторового аналізу є важливим компонентом забезпечення безпеки критичних об'єктів. Зокрема, оперативний супутниковий геомоніторинг наслідків руйнування Каховської ГЕС показав ефективність використання супутникових даних для аналізу кризових ситуацій [6]. Аналогічно, використання супутникових кластерів Ionosats дозволяє покращити спостереження за станом іоносфери та потенційними загрозами [7]. Застосування методів супутникового агромоніторингу є перспективним підходом до контролю стану земної поверхні, виявлення загроз для сільського господарства та моніторингу критичної інфраструктури [8], [9].

Постановка завдання. Таким чином, метою роботи є аналіз методів таргетованих атак на супутникові інтернет-системи, оцінка їхнього впливу та розробка рекомендацій щодо кіберзахисту. Досліджуються вразливості Starlink, відомі випадки атак із застосуванням шкідливого ПЗ та методи компрометації мережевої інфраструктури. Оцінюється ефективність традиційних систем кібербезпеки у протидії сучасним загрозам. Пропонується концепція емерджентно-адаптивної нейромережі для виявлення та блокування атак у режимі реального часу. Обґрунтовується інтеграція міжнародних стандартів кібербезпеки, зокрема ДСТУ ISO/IEC 27001:2023, для підвищення стійкості супутникових мереж.

Виклад основного матеріалу. Сучасні кібератаки є складними, багатоетапними процесами, які потребують ретельного планування, координації та адаптації до змінних умов. У цьому дослідженні розглядається алгоритм атак (рис.1), застосовуваний групою Secret Blizzard, яка здійснює таргетовані кібератаки на інформаційні системи, зокрема на ті, що використовують супутниковий інтернет Starlink. Представлений алгоритм є циклічним та гнучким, що дозволяє зловмисникам швидко пристосовуватися до нових контрзаходів і змінювати стратегії для досягнення своїх цілей.

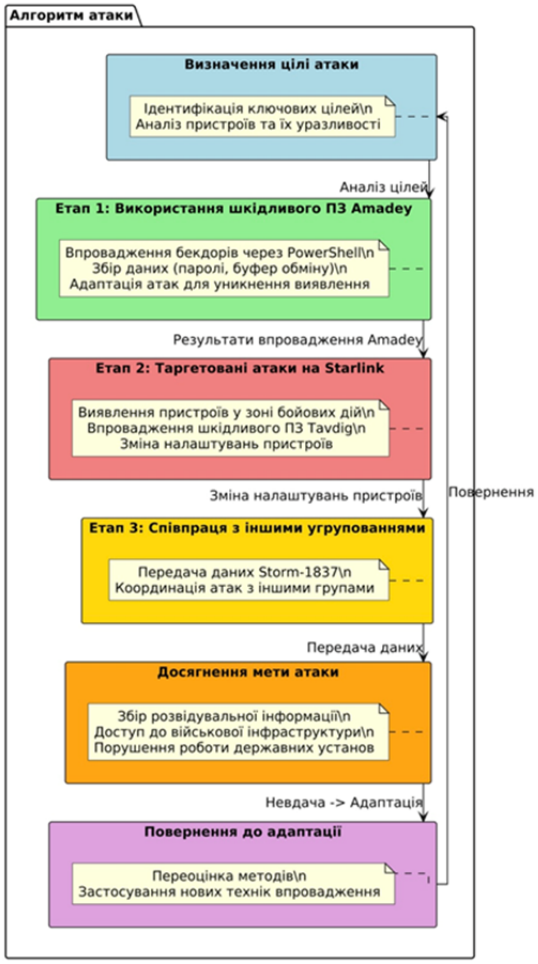

Рисунок 1 – Етапи алгоритму атаки

Джерело: розроблено авторами

Визначення цілі атаки

На початковому етапі здійснюється ідентифікація ключових цілей, зокрема інформаційних систем, що працюють через Starlink. Аналізується вразливість пристроїв для подальшого планування атаки.

Етап 1: Використання шкідливого ПЗ Amadey

Впроваджується шкідливе програмне забезпечення Amadey через PowerShell-скрипти та дроппери. Основними завданнями цього етапу є встановлення бекдорів для віддаленого доступу, збір чутливих даних (паролі, буфер обміну) та адаптація атак для обходу антивірусного захисту.

Етап 2: Таргетовані атаки на Starlink

Виконується пошук пристроїв у зоні бойових дій, після чого на них впроваджується шкідливе ПЗ Tavdig. Це дозволяє зловмисникам змінювати конфігурацію обладнання, що може призвести до збоїв або повної зупинки його роботи.

Етап 3: Співпраця з іншими угрупованнями

Зібрані дані передаються угрупованню Storm-1837, яке спеціалізується на відстеженні операторів дронів та військових комунікацій. Також здійснюється координація атак з іншими хакерськими групами для підвищення ефективності дій.

5. Досягнення мети атаки

Головними завданнями атак є:

Отримання розвідувальної інформації щодо діяльності ЗСУ.

Доступ до ключових компонентів військової інфраструктури.

Дестабілізація роботи державних установ.

6. Повернення до адаптації

У разі, якщо атака не досягла своїх цілей, алгоритм повертається на початковий етап. Проводиться переоцінка методів, впроваджуються нові техніки атак, адаптовані до виявлених контрзаходів. Запропонований алгоритм атак демонструє високу ступінь організованості та координації дій угруповання Secret Blizzard. Гнучкість і адаптивність їхніх атак дозволяють їм ефективно протистояти системам захисту, що робить їх надзвичайно небезпечними для інформаційних систем і критичної інфраструктури.

Математична модель виявлення атак та її використання в емерджентно адаптивних нейромережах кібербезпеки

Постановка задачі

у системі кіберзахисту є множина можливих загроз $\{T_1, T_2, \dots, T_n\}$. Для кожної загрози T_i визначено:

- ймовірність виникнення загрози $\mathrm{p_i}$ (за статистикою чи аналітикою);
- ваговий коефіцієнт $\mathrm{w_i}$, що відображає важливість та критичність загрози;
- функція виявлення (активності) $f_i(x)$, що залежить від вхідних даних моніторингу x (наприклад, трафік, логи, поведінкові ознаки).

Математична модель виявлення атак

Інтегральну ймовірність наявності атаки (або сумарний рівень загрози) можна представити у вигляді:

$$P_{\text{attack}} = \sum_{i=1}^{n} w_i p_i f_i(x) \#(1),$$

тут $p_i \sim -$ імовірність появи -тої загрози;

$w_i^{i\text{-тої загрози;}} \sim -$ ваговий коефіцієнт критичності;

$f_i(x) \sim -$ функція, що повертає (зазвичай у діапазоні $[0,1]$) рівень впевненості у наявності загрози T_i на основі поточних даних x.

Алгоритм оцінки ризику (CIA-параметри)

У класичній триаді безпеки конфіденційність, цілісність, доступність задаються:

$$P_C, P_I, P_A$$

де P_C – рівень (ймовірність) збереження конфіденційності;

$P_{I\sim} -$ рівень (ймовірність) збереження цілісності;

$P_{A\sim}$ – рівень (ймовірність) збереження доступності.

Базова формула для рівня ризику

Найчастіше інтергальний рівень ризику R беруть як імовірність порушення принаймні одного з параметрів C, I, A :

$$R = 1 - (P_C \times P_I \times P_A) \#(2)$$

Якщо відомі вагові коефіцієнти $\alpha_C, \alpha_I, \alpha_A$, що відображають різну важливість складових (за умови $\alpha_C + \alpha_I + \alpha_A = 1$), можна використовувати альтернативний варіант:

$$R = \alpha_C(1 - P_C) + \alpha_I(1 - P_I) + \alpha_A(1 - P_A)$$

Приклад із заданими параметрами

Припустимо, що маємо такі значення (згідно з Таблицею~1 дослідження):

$$P_C = 0.95, P_I = 0.90, P_A = 0.85$$

Тоді, скориставшись формулою (2):

$$R = 1 - (0.95 \times 0.90 \times 0.85) = 1 - 0.72675 \approx 0.27325$$

Отже, сумарний ризик складає приблизно 27,3%.

Застосування в емерджентно адаптивних нейромережах

Емерджентність

Емерджентна поведінка означає, що складна нейромережа, взаємодіючи з великою кількістю вхідних даних і внутрішніх елементів, може виявляти нові закономірності (наприклад, zero-day атаки або нестандартні сценарії) без жорстко визначеного алгоритму.

Адаптивність

Адаптивна нейромережа здатна дінамічно коригувати вагові коефіцієнти $\boldsymbol{w_i}$ у формулі (1) та оновлювати функції виявлення $\boldsymbol{f_i(x)}$ під впливом:

- змін у профілі загроз (нові вразливості, нові типи атак);
- результатів аналізу вхідних сигналів (трафік, логи, поведінкові патерни);
- зворотного зв'язку від спеціалістів з кібербезпеки (підтверджені атаки чи хибні спрацьовування).

Переваги використання нейромережі

Проактивне виявлення атак: зниження ризику невчасного реагування, оскільки мережа навчається на великих обсягах даних та виявляє приховані патерни.

Зменшення хибних спрацьовувань: адаптивне налаштування порогу спрацювання та індивідуальна корекція вагових коефіцієнтів.

Оцінка ризику в реальному часі: підрахунок $\boldsymbol{R}$ з формули (2) чи (3) з урахуванням актуальних даних дає змогу автоматично активувати додаткові заходи кіберзахисту.

Висновок

Запропонована математична модель виявлення атак у вигляді:

$$P_{\text{attack}} = \sum_{i=1}^{n} w_i p_i f_i(x),$$

та використання показника ризику

$$R = 1 - (P_C \times P_I \times P_A)$$

(або його зваженого аналога) можуть бути ефективно реалізовані в емерджентно адаптивних нейромережах кібербезпеки.

Адаптивність дає можливість постійно підлаштовуватися до нових загроз, змінюючи ваги та пороги спрацювання в режимі реального часу. Це істотно підвищує загальний рівень захисту, знижує кількість хибних спрацьовувань та забезпечує інтегровану оцінку ризиків з урахуванням факторів конфіденційності, цілісності й доступності.

Обговорення. Проведений аналіз таргетованих атак на супутникові інтернет-системи показав високий рівень координації дій зловмисників та використання багаторівневих методів ураження. Атаки групи Secret Blizzard базувалися на використанні шкідливого програмного забезпечення Amadey і Tavdig, що дозволило обійти традиційні системи кіберзахисту. Крім того, зловмисники застосовували PowerShell-дроппери та змінювали конфігурацію мережевих пристроїв, що суттєво підвищувало ефективність атак.

Висновки. Таргетовані атаки на супутникові інтернет-системи, такі як Starlink, є складними та багаторівневими, що ускладнює їх виявлення. Зловмисники використовують сучасні техніки, зокрема Amadey і Tavdig, що дозволяє їм досягати високої ефективності. Традиційні системи кіберзахисту не відповідають сучасним викликам, через що стають малоефективними. Емерджентно-адаптивні нейромережі показали високу ефективність у скороченні часу реакції та підвищенні точності виявлення атак. Інтеграція таких рішень з міжнародними стандартами, як-от ДСТУ ISO/IEC 27001:2023, забезпечує формалізацію та підвищення стійкості систем кіберзахисту. Впровадження емерджентно-адаптивних технологій дозволить створити надійний захист супутникових інтернет-систем, зменшити ризики атак і підвищити стійкість критичної інфраструктури до сучасних кіберзагроз.

Список літератури

1. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Система керування інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2023. 12 с.
2. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Код практики для заходів контролю інформаційної безпеки. Київ: ДП «УкрНДНЦ», 2023. 21 с.
3. НАТО STANAG 4586. Стандарт взаємодії систем управління безпілотними авіаційними комплексами. Брюссель: НАТО, 2023. 34 с.
4. Наказ Державного центру кіберзахисту Держспецзв'язку України № 79 від 10.11.2021. Правила обміну інформацією про кіберінциденти та перелік категорій кіберінцидентів. Київ: Держспецзв'язку, 2021. 22 с.
5. Наказ Адміністрації Держспецзв'язку України № 773 від 30.08.2023. Методичні рекомендації щодо підвищення рівня кібербезпеки систем електронного документообігу. Київ: Держспецзв'язку, 2023. 15 с.
6. Ліщенко Л. П., Філіпович В. Є. Оперативний супутниковий геомоніторинг наслідків руйнування греблі Каховської гідроелектростанції. Ukrainian Journal of Remote Sensing. 2024. Т. 11, № 1. С. 14–20. DOI: 10.36023/ujrs.2024.11.1.25.
7. Ivchenko V. M., Korepanov V. Ye., Lizunov G. V., Fedorov O. P., Yampolski Yu. M. The ionospheric satellite cluster Ionosats. Kosmična nauka i tehnologiya. 2007. Т. 13, № 3. С. 55–66. DOI: 10.15407/knit2007.03.055.
8. Kussul N., Shelestov A., Kolotii A., Lavreniuk M., Butko I. Satellite agromonitoring in Ukraine. Visnik Nacional'noi akademii nauk Ukraini. 2016. № 2. С. 96–102. DOI: 10.15407/visn2016.02.096.
9. Shelestov A. Yu., Yailymov B. Ya., Yailymova H. O., Bilokonska Y. V., Nivievskyi O. V. Satellite crop monitoring for Ukraine. Kosmična nauka i tehnologiya. 2020. Т. 26, № 6. С. 27–37. DOI: 10.15407/knit2020.06.027.
10. Wang B., Kharchenko V., Grekhov A., Ali I. Оцінювання умов перевантаження при передаванні даних через супутниковий канал зв'язку. Вісник Національного авіаційного університету. 2016. Т. 66, № 1. DOI: 10.18372/9865.
11. Kavats O., Kavats Y., Dibrii D. Супутниковий моніторинг оцінки стану забруднення водних об'єктів на основі машинного навчання. International Scientific and Technical Conference Information Technologies in Metallurgy and Machine Building. 2024. С. 495–499. DOI: 10.34185/1991-7848.itmm.2024.01.095.
12. Ліщенко Л. П. Супутниковий моніторинг стану геосистеми локального рівня на прикладі Матвіївського лісу поблизу м. Миколаїв (Україна). Ukrainian Journal of Remote Sensing. 2023. Т. 10, № 2. С. 27–34. DOI: 10.36023/ujrs.2023.10.2.22.
13. Dudnik O. V. Satellite telescope of electrons and protons STEP-F of the space scientific project CORONAS-PHOTON. Visnik Nacional'noi akademii nauk Ukraini. 2017. Т. 11. С. 53–65. DOI: 10.15407/visn2017.11.053.
14. Kussul N. M., Shelestov A. Yu., Lavreniuk M. S., Kolotii A. V., Yailymov B. Ya., Yailymova G. O. Satellite agromonitoring in Ukraine: Results of Sentinel-2 for agriculture project and further prospects. Visnik Nacional'noi akademii nauk Ukraini. 2016. № 12. С. 99–104. DOI: 10.15407/visn2016.12.099.

References

1. DSTU ISO/IEC 27001:2023. (2023). Information security, cybersecurity and privacy protection. Information security management system. Requirements. Kyiv: DP 'UkrNDNC'.
2. DSTU ISO/IEC 27002:2023. (2023). Information security, cybersecurity and privacy protection. Code of practice for information security controls. Kyiv: DP 'UkrNDNC'.
3. NATO STANAG 4586. (2023). Standard for interoperability of unmanned aerial vehicle control systems. Brussels: NATO.
4. State Cyber Protection Center of the State Special Communications Service of Ukraine. (2021). Order No. 79 of 10.11.2021. Rules for exchanging information on cyber incidents and the list of categories of cyber incidents. Kyiv: State Special Communications Service.
5. Administration of the State Special Communications Service of Ukraine. (2023). Order No. 773 of 30.08.2023. Methodological recommendations for improving the level of cybersecurity of electronic document management systems. Kyiv: State Special Communications Service.
6. Lishchenko, L. P., & Filipovych, V. Ye. (2024). Operational satellite geomonitoring of the consequences of the destruction of the Kakhovka Hydroelectric Power Plant dam. *Ukrainian Journal of Remote Sensing,* 11(1), 14–20. https://doi.org/10.36023/ujrs.2024.11.1.25

7. Ivchenko, V. M., Korepanov, V. Ye., Lizunov, G. V., Fedorov, O. P., & Yampolski, Yu. M. (2007). The ionospheric satellite cluster Ionosats. *Kosmična nauka i tehnologiya,* 13(3), 55–66. https://doi.org/10.15407/knit2007.03.055
8. Kussul, N., Shelestov, A., Kolotii, A., Lavreniuk, M., & Butko, I. (2016). Satellite agromonitoring in Ukraine. *Visnik Nacional'noi akademii nauk Ukraini,* (2), 96–102. https://doi.org/10.15407/visn2016.02.096
9. Shelestov, A. Yu., Yailymov, B. Ya., Yailymova, H. O., Bilokonska, Y. V., & Nivievskyi, O. V. (2020). Satellite crop monitoring for Ukraine. *Kosmična nauka i tehnologiya,* 26(6), 27–37. https://doi.org/10.15407/knit2020.06.027
10. Wang, B., Kharchenko, V., Grekhov, A., & Ali, I. (2016). Evaluation of overload conditions during data transmission via satellite communication channels. *Visnyk of the National Aviation University,* 66(1). https://doi.org/10.18372/9865
11. Kavats, O., Kavats, Y., & Dibrii, D. (2024). Satellite monitoring of water pollution assessment using machine learning. International Scientific and Technical Conference on Information Technologies in Metallurgy and Machine Building, 495–499. https://doi.org/10.34185/1991-7848.itmm.2024.01.095
12. Lishchenko, L. P. (2023). Satellite monitoring of the local geosystem state on the example of Matviyivskyi Forest near Mykolaiv (Ukraine). *Ukrainian Journal of Remote Sensing*, 10(2), 27–34. https://doi.org/10.36023/ujrs.2023.10.2.22
13. Dudnik, O. V. (2017). Satellite telescope of electrons and protons STEP-F of the space scientific project CORONAS-PHOTON. *Visnik Nacional'noi akademii nauk Ukraini,* (11), 53–65. https://doi.org/10.15407/visn2017.11.053
14. Kussul, N. M., Shelestov, A. Yu., Lavreniuk, M. S., Kolotii, A. V., Yailymov, B. Ya., & Yailymova, G. O. (2016). Satellite agromonitoring in Ukraine: Results of Sentinel-2 for agriculture project and further prospects. *Visnik Nacional'noi akademii nauk Ukraini,* (12), 99–104. https://doi.org/10.15407/visn2016.12.099

Dmytro Prokopovych-Tkachenko, Assoc. Prof., PhD , tech. sci.
Customs and Finance University, Dnipro, Ukraine
Volodymyr Zverev, Assoc. Prof., PhD , tech. sci., **Valeriy Bushkov,** post-graduate
State University of Trade and Economics, Kyiv, Ukraine
Borys Khrushkov, post-graduate, **Oleksandr Cherkaskiy, s**tudent
Customs and Finance University, Dnipro, Ukraine

Targeted Attacks on Satellite Internet Systems: Challenges and Protection Approaches

The purpose of this article is to analyze modern targeted cyberattacks on satellite internet systems, assess their impact on critical infrastructure, and develop recommendations for enhancing cybersecurity measures. The study focuses on identifying vulnerabilities within the Starlink system, widely used in remote areas and military operations. Given the increasing complexity of cyber threats, traditional protection methods prove ineffective against multi-vector attacks, emphasizing the necessity of adaptive defense mechanisms. The paper proposes an innovative approach based on emergent-adaptive neural networks, which can dynamically monitor and respond to cyber threats in real time. Furthermore, the integration of international cybersecurity standards, such as DSTU ISO/IEC 27001:2023, is considered essential for strengthening the resilience of satellite communication networks.

The research thoroughly examines documented cyber incidents targeting Starlink, highlighting the use of advanced malware like Amadey and Tavdig, as well as techniques such as PowerShell droppers and network configuration manipulation. The study details the attack cycle, including reconnaissance, payload deployment, data extraction, and system destabilization. The effectiveness of traditional cybersecurity measures is critically assessed, revealing their limitations in mitigating sophisticated cyber threats. To counteract these challenges, a multi-layered defense system based on emergent-adaptive neural networks is proposed.

The findings indicate that modern cyber threats targeting satellite communication systems require a paradigm shift in cybersecurity strategies. The proposed adaptive neural network approach improves the ability to identify and neutralize cyber threats in real time, offering a more resilient and efficient protection mechanism. Additionally, compliance with international cybersecurity standards is highlighted as a key factor in maintaining a robust security framework. Future research should explore the integration of AI-driven cybersecurity solutions with existing satellite monitoring and defense infrastructures, ensuring comprehensive protection against emerging cyber threats.

cybersecurity, satellite internet, Starlink, malware, targeted attacks, neural networks, PowerShell droppers

Одержано (Received) 18.11.2024 *Прорецензовано (Reviewed) 18.12.2024*
Прийнято до друку (Approved) 23.12.2024