https://doi.org/10.31891/2219-9365-2022-71-3-9
УДК 004.77

ЮРІЙ КЛЬОЦ
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
klots@khmnu.edu.ua
НАТАЛІЯ ПЕТЛЯК
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
npetlyak@khmnu.edu.ua

ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ У ЗАГАЛЬНОДОСТУПНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

В статті проведено аналіз статистик Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України по кількісному та якісному складу атак, та звітів IBM по збиткам, що вони завдали. Проаналізовано системи контролю та аналізу трафіку, визначено загальну направленість таких засобів на виявлення атак на мережу. Визначено типи атак, що зазвичай проводяться з ЗКМ та дано опис їх дій. Представлено архітектуру загальнодоступних комп'ютерних мереж (ЗКМ), визначено її складові, місце зловмисника та системи захисту. Показано, що типове місце зловмисника за межами мережі не відповідає дійсності саме для ЗКМ. Запропоновано структуру ЗКМ, яка дозволяє захищати мережу як від зовнішніх так і від внутрішніх зловмисників.

Ключові слова: загальнодоступна комп'ютерна мережа, аномалії, кіберінциденти, атаки, мережевий трафік, система виявлення аномального трафіку.

YURII KLOTS, NATALIIA PETLIAK
Khmelnytskyi National University

ANOMALOUS TRAFFIC DETECTION IN PUBLIC COMPUTER NETWORKS

The increase in the number of users of Internet services and the digitization of society leads to a rapid increase in traffic volumes, and computer networks are increasingly becoming targets of cyber attacks. Which negatively affects the functioning and causes damage in various public or private spheres of activity.

The article analyzes the statistics of the State Center for Cyber Protection of the State Service for Special Communications and Information Protection of Ukraine on the quantitative and qualitative composition of attacks, and IBM reports on the damage they caused. Traffic control and analysis systems were analyzed, and the general orientation of such means for detecting attacks on the network was determined. The types of attacks that are usually carried out with ZKM are defined and a description of their actions is given. The architecture of public computer networks (PCNs) is presented, its components, location of the attacker and protection systems are defined. It is shown that the typical location of the attacker outside the network does not correspond to the reality, especially for ZKM. The structure of ZKM is proposed, which allows to protect the network from both external and internal attackers.

Keywords: public computer network, anomalies, cyber incidents, attacks, network traffic, anomalous traffic detection system.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Збільшення користувачів Інтернет-послуг та цифровізація суспільства призводить до стрімкого збільшення об'ємів трафіку, а комп'ютерні мережі все частіше стають об'єктами кібератак. Що негативно впливає на функціонування та завдає шкоди у різних державних чи приватних сферах діяльності.

Проблема виявлення аномального трафіку має недостатню кількість рішень. Відомі системи виявлення вторгнень [1-4] орієнтовані на виявлення атак на корпоративні мережі, та не націлені на виявлення атак, що виходять із загальнодоступних комп'ютерних мереж (ЗКМ) та використовують їх потужності для атак на третіх осіб.

Аналіз досліджень та публікацій

Оперативним центром реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України було опубліковано звіти роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 1кв. [5] та 2кв. [6] 2022 року. Дана система функціонувала із об'єктами, що визначено у Порядку функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, що затверджено кабінетом міністрів України від 23 грудня 2020 року [7], зокрема з обласними військовими адміністраціями та ЗВІД [8].

Згідно даного звіту у другому кварталі опрацьовано на 37,2% менше критичних подій інформаційної безпеки (рис.1). Це пов'язано в першу чергу із тим, що постачальники електронних комунікаційних мереж та/або послуг, які забезпечують доступ до інтернету, заблокували IP-адреси, що використовуються рф.

ISSN 2219-9365

Також потрібно враховувати, що частина сервісів перестала функціонувати з тих чи інших обставин. Проте кіберінцидентів зареєстровано на 60% більше (рис. 2).

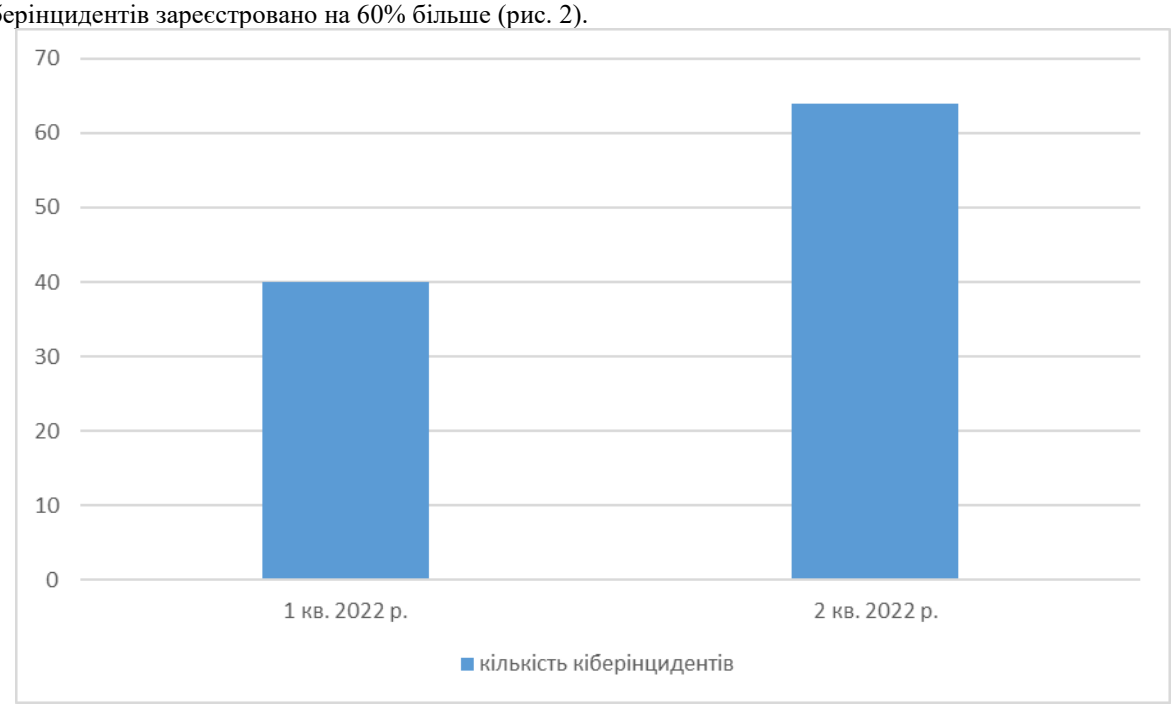

Рис. 1. Кількості зафіксованих кіберінцидентів у 2кв. 2022 року в порівнянні з 1кв. 2022 року

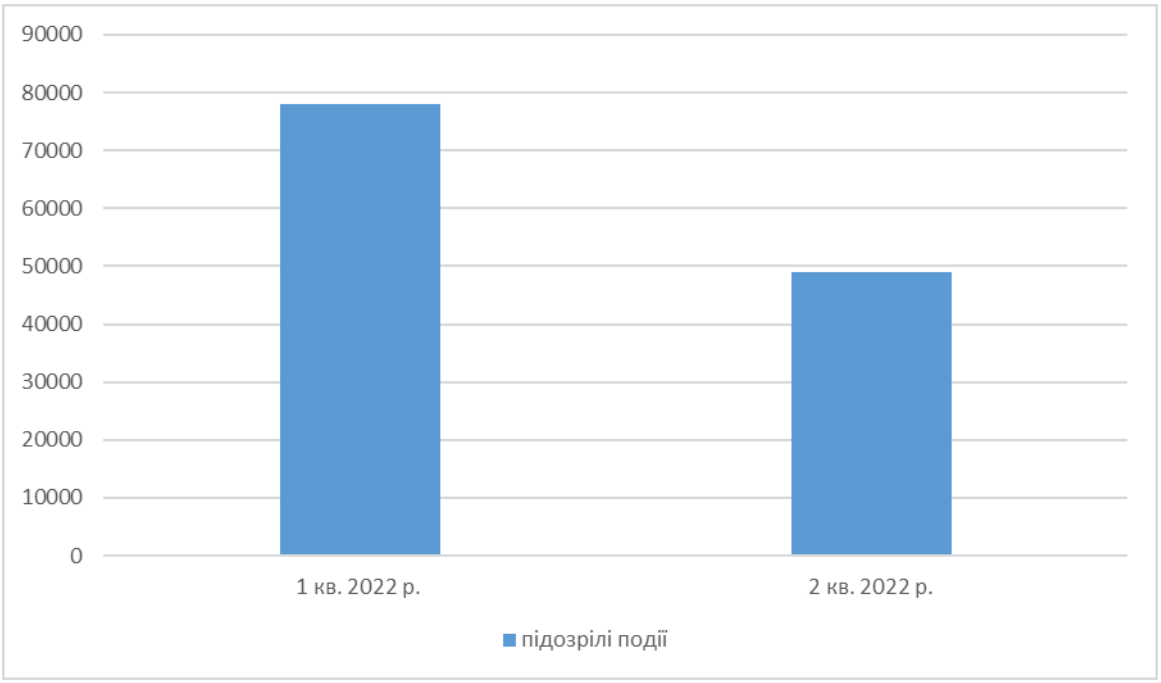

Рис. 2. Кількості підозрілих подій у 2кв. 2022 року в порівнянні з 1кв. 2022 року

Згідно звіту [6] протягом 2кв. 2022 року на 38% у порівнянні з попереднім кварталом зросла кількість подій інформаційної безпеки в категорії «Шкідливий програмний код». Це свідчить про підвищення рівня шкідливої мережевої активності, зокрема залучення нових чи експлуатація раніше інфікованих пристроїв бот-мереж.

У звіті IBM за 2022 рік [9] вказано, що середня вартість порушень у США найвища з усіх країн та становить 9,44млн.дол. На рис 3 представлено середню вартість витоку даних, де вартість для критичної інфраструктури становить 4,82млн.дол., а 3,83млн.дол. вартість для організацій некритичної інфраструктури: розваги, споживчі товари, роздрібна торгівля та інше.

У порівнянні з аналогічним періодом 2021 року кількість DoS-атак (та DDoS-атак) зросла в 4,5 рази [10].

Статистика стрімкого розвитку фішингових атак представлена на рис.4 [11].

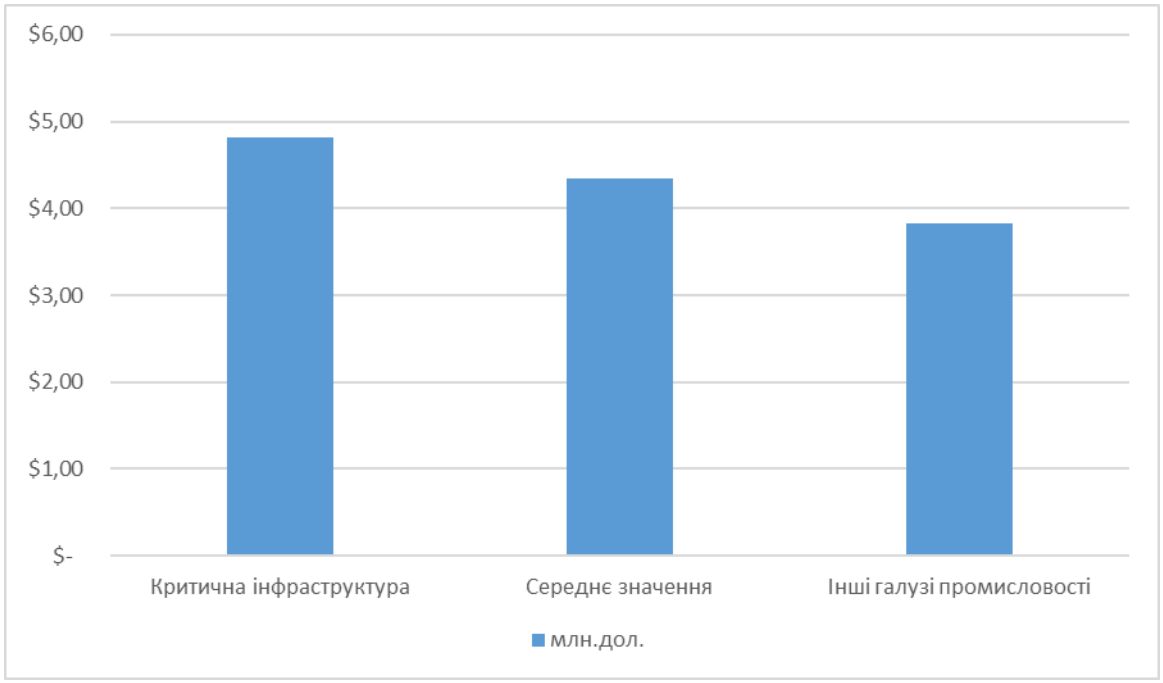

Рис. 3. Вартості витоку даних

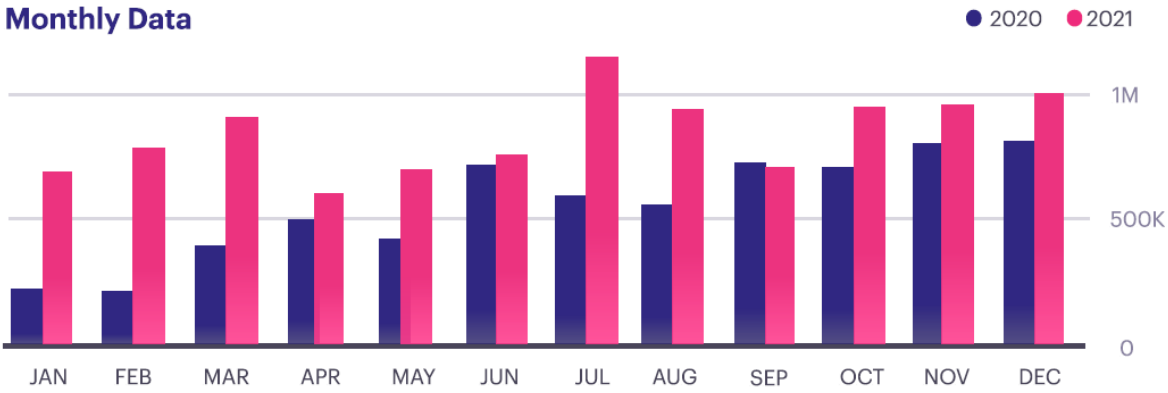

Рис. 4. Фішингові атаки з січня 2020 року по грудень 2021

Отож, кількість атак та їх характер суттєво збільшилась у порівнянні з попередніми роками [12]. Саме тому слід дбати про безпеку мережі задля своєчасного виявлення вторгнень.

Формулювання цілей статті

ЗКМ переважно використовують у громадських місцях для забезпечення доступу до мережі Інтернет для відвідувачів кафе, торгових центрів тощо. Дана можливість збільшує кількість відвідувачів за рахунок незначних капіталовкладень. Підключення до такої мережі може здійснити будь-яка особа без ідентифікації. Це, в свою чергу, дозволяє зловмиснику додатково приховати себе при виконанні зловмисних дій. Задоволення потреби клієнта в анонімному доступі до ЗКМ дозволяє зловмиснику підвищити рівень анонімності при проведенні атак на сторонні ресурси.

Задача дослідження полягає у розробці нових методів та засобів, що одночасно можуть забезпечити безпеку ЗКМ та, з відповідним рівнем достовірності, не допускатимуть зловмисних дій користувачів цієї мережі по відношенню до третіх осіб. Оскільки відомі методи та засоби захисту мереж не забезпечують вирішення таких задач.

Вирішення поставлених задач дозволить зменшити загальну кількість атак у мережах та зменшити трафік у власній мережі.

Виклад основного матеріалу

Перелік категорій кіберінцидентів розроблений на основі Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони

України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021) [13]. До нього відносять:

- шкідливий вміст: основним типом інцидентів є спам під час якого відбувається розсилка великої кількості небажаних повідомлень;
- шкідливий програмний код: частими інцидентами є виявлення та розповсюдження шкідливого програмного забезпечення, використання ботнету чи шкідливі підключення;
- збір інформації: найпоширенішими прикладами є фішинг, несанкціонований аналіз мережевого трафіку та збір інформації про стан мережі;
- спроби втручання: до інцидентів цього типу відносять спроби входу з використанням раніше скомпрометованих даних чи підбору аутентифікаційних даних або ж спроба вторгнення з використанням вразливостей мережі;
- втручання: вторгнення в систему шляхом компрометації системи чи облікового запису;
- порушення доступності: кіберінциденти найчастіше видно пересічному користувачеві, оскільки відбувається відмова в обслуговуванні (DoS/DDoS), зміна чи видалення даних, збій в роботі системи;
- порушення властивостей інформації: несанкціонований обмін чи зміна інформації;
- шахрайство: переважно створення фішингових сайтів для збору персональних даних;
- відомі вразливості: недоліки в налаштуванні системи чи використання відомих вразливостей у системі;
- інше, що не вдалось обробити для визначення кіберінциденту через брак інформації.

Ідентифікація зловмисного трафіку та аномалій відіграє важливу роль для безпеки. Тому потрібно використовувати системи виявлення вторгнень (СВВ, Intrusion Detection System, IDS), які можуть захистити мережу від існуючих та майбутніх загроз. IDS забезпечують вчасне оповіщення адміністраторів системи.

Згідно звіту [14] найпоширенішими є спроби втручання та збір інформації зловмисником, а 33% подій не вдалось обробити через брак даних про подію. Проте вже у 1кв. 2022 року відбувся перерозподіл по рейтингу за кількістю подій того чи іншого типу. Зокрема 34% подій становить шкідливий програмний код, спроби втручання зменшились на 3% та збір інформації зловмисником збільшився на 2%. А кількість подій, що не вдалось обробити через брак даних про подію, зменшилась до 2%. Наглядну статистику приведено на рис.5 та рис.6.

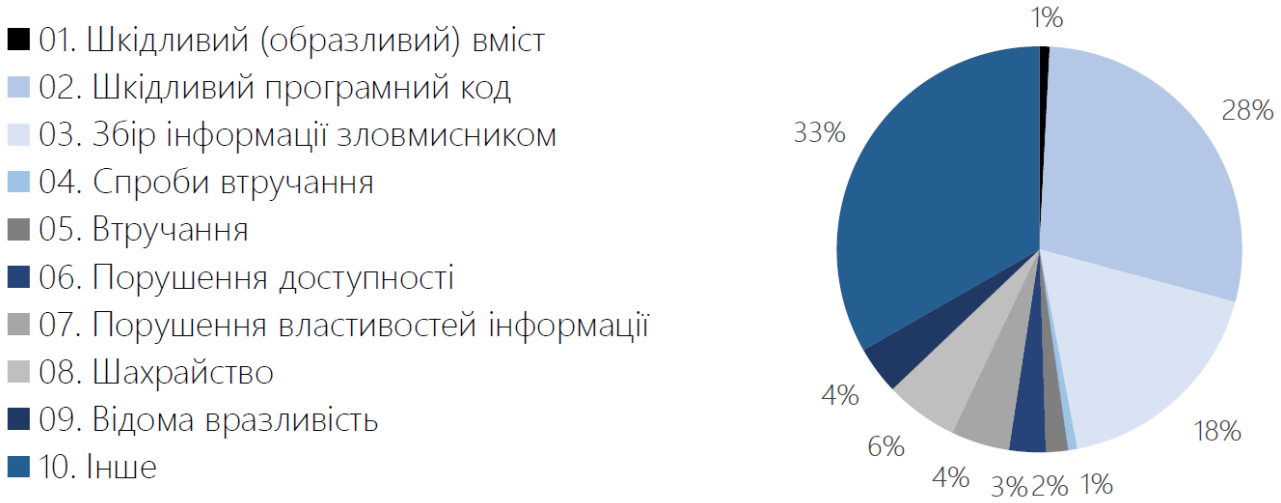

Рис. 5. Статистика кіберінцидентів з поділом на категорії за 2021рік, де 100% дорівнює ≈160тис. опрацьованих критичних подій

Розглянемо поширені типи атак у ЗКМ та опис їх роботи.

Атака на відмову в обслуговуванні (DoS) – це атака, спрямована на надмірне перевантаження комп'ютера або мережі, що робить їх недоступними для призначених користувачів. DoS-атаки досягають цього, переповнюючи ціль трафіком або надсилаючи їй інформацію, яка викликає збій.

Існує два загальні методи DoS-атак: перевантаження служб або збій служб. До популярних атак належать:

- Атаки переповнення буфера - найпоширеніша DoS-атака. Концепція полягає в тому, щоб відправити на мережеву адресу більше трафіку, ніж система може опрацювати.
- ICMP-флуд - використовує неправильно налаштовані мережеві пристрої, надсилаючи підроблені пакети, які перевіряють пінг на кожному комп'ютері цільової мережі, а не лише на одному конкретному комп'ютері. Ця атака також відома як атака смурфа або пінг смерті.

- SYN flood - надсилає запит на підключення до сервера, але ніколи не завершує рукостискання. Триває, доки всі відкриті порти не будуть переповнені запитами, і жоден з них не стане доступним для підключення законних користувачів.

Злом паролів – це процес використання прикладної програми для визначення невідомого або забутого пароля до комп'ютера чи мережевого ресурсу. Застосовують для того, щоб допомогти зловмиснику отримати несанкціонований доступ до ресурсів.

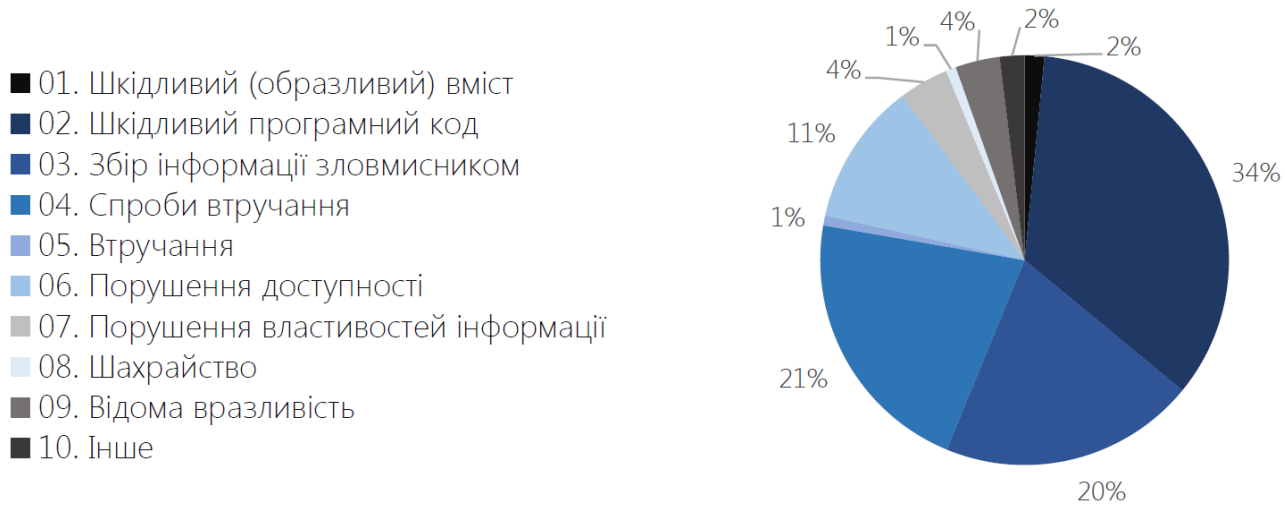

Рис. 6. Статистика кіберінцидентів з поділом на категорії за 1 квартал 2022 року, де 100% дорівнює ≈78тис. опрацьованих критичних подій

Фішинг використовується шахраями, що видають себе за довірених осіб, для виманювання персональних даних. Це може досягатися шляхом проведення масових розсилок електронних листів від імені популярних брендів. Також проявами фішингу можуть бути спливаючі вікна, що з'являються на сайтах, яким довіряють користувачі.

Паролі часто є слабкою ланкою в кібербезпеці організації чи окремої людини. Фактично, для базових атак на веб-додатки (BWAA) понад 80% зломів можна пояснити викраденими обліковими даними. Середньостатистичний користувач Інтернету має 240 облікових записів, які потребують пароля [15].

Відповідно до рис.7, у 2021 році найчастіше було виявлено сканування мережі, порушення мережевої політики безпеки та витік даних. Найрідше виявляли з'єднання з командно-контрольними серверами та компрометацію даних [14].

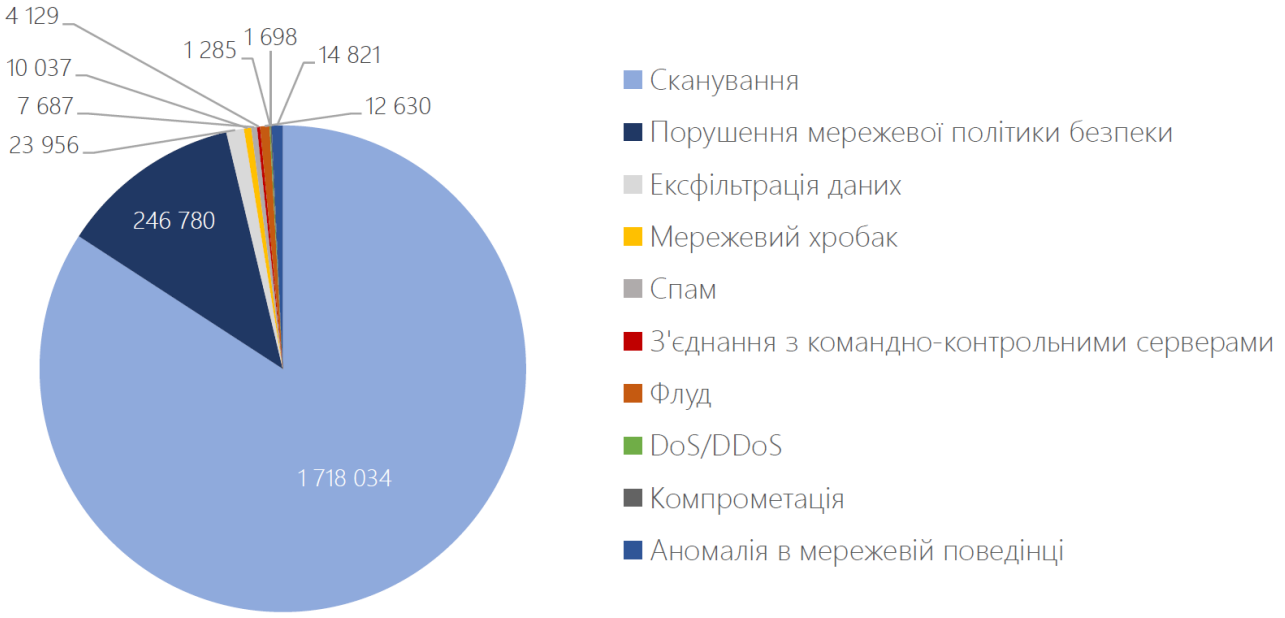

Рис. 7. Категорії детектувань на основі поведінкового аналізу у 2021 році

Усі з перерахованих атак виконуються з використанням ресурсів віддалених комп'ютерних систем, які, зазвичай, допомагають приховати зловмисника.

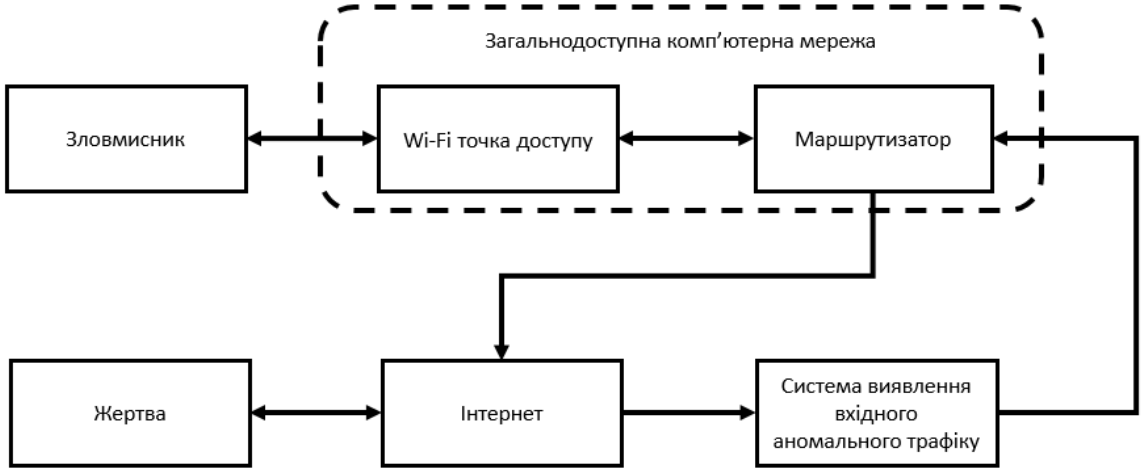

Рис. 8. Структура ЗКМ з використанням системи виявлення вхідного аномального трафіку

Типове представлення їх роботи зображено на рис.8. Довільний пристрій може приєднатися до ЗКМ через Wi-Fi точку доступу, яка у більшості випадків не має пароля для доступу. Далі зловмисник може робити спроби несанкціонованого доступу чи злому третіх осіб користуючись ресурсами ЗКМ. У такому випадку буде здійснено компрометацію мережі, а безпосередньо зловмисника неможливо визначити. З розвитком різноманітних мережевих атак все більше користувачів дбає про безпеку власної мережі та використовує системи виявлення аномального трафіку, проте вони відслідковують лише вхідні дані з метою захисту КМ від несанкціонованого доступу чи злому. У той же час не аналізується вихідний трафік.

Розглянемо відомі IDS та їх функціональні можливості.

Snort - це система виявлення вторгнень у мережу з відкритим кодом, здатна виконувати аналіз трафіку в реальному часі та реєструвати пакети в IP-мережах. Snort складається з двох основних компонентів: механізму виявлення і гнучкої мови правил для опису трафіку. Для використання Snort діє ліцензія GNU General Public License Version 2, а для використання власних правил - ліцензія Non-Commercial Use License for the Proprietary Snort® Rules [16]. Працює на ОС Windows, Linux та Unix.

Wireshark - це аналізатор мережевих протоколів. Він дозволяє фіксувати та інтерактивно переглядати трафік, що пересилається в комп'ютерній мережі, має багатий і потужний набір функцій і є найпопулярнішим у світі інструментом такого роду. Він працює на більшості комп'ютерних платформ, включаючи Windows, macOS, Linux і UNIX. Професіонали з мереж, експерти з безпеки, розробники та викладачі в усьому світі регулярно використовують його. Він є у вільному доступі у відкритому доступі та випущений під GNU General Public License Version 2 [17].

Інструмент Network Monitor, реалізований у Windows та Microsoft Systems Management Server (SMS), дозволяє виконувати моніторинг мережевого трафіку. Моніторинг можна проводити в реальному часі або, перехопивши і зберігши мережевий трафік, аналізувати його пізніше.

Suricata - це високопродуктивне програмне забезпечення для аналізу мережі та виявлення загроз із відкритим кодом, яке використовується більшістю приватних і державних організацій і впроваджується великими постачальниками для захисту своїх активів. Для використання Suricata діє ліцензія GNU General Public License Version 2 [18].

Security Onion класифікується як безкоштовна система виявлення мережевих атак (Network Intrusion Detection System, NIDS), але він також включає функції хостової IDS (Host-based intrusion detection system, HIDS). Система створена для операційної системи Linux з акцентом на управління журналами, моніторингом безпеки підприємства та виявлення атак.

Огляд методів навчання IDS описано у [19]. Усі вони орієнтовані на захист поточної мережі від атаки. І не пристосовані для недопущення атак, що виходять за межі цієї мережі.

Рис. 9. Структура ЗКМ із використанням системи виявлення вихідного аномального трафіку

Саме тому на рис.9 представлено структуру із використанням системи виявлення вихідного аномального трафіку. Дана система виявлятиме аномальний трафік, фіксуватиме користувача від якого надходить даний трафік і блокуватиме його. Одночасно з блокуванням буде надходити сповіщення для адміністратора мережі про зафіксований інцидент. Адміністратор буде бачити звіт про функціонування системи в реальному часі або ж переглядати в лог-файлах за потреби. Блокування аномального вихідного трафіку забезпечуватиме зменшення кількості мережевих атак та зменшення навантаження на мережу й обладнання, надаватиме захист від компрометації мережі.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В ході проведеного дослідження виявлено значну кількість атак, що відбуваються в комп'ютерних мережах. Також визначено, що чимала частина атак відбувається з ЗКМ. В свою чергу відомі методи захисту КМ націлені на виявлення атак на мережу. Використання ЗКМ для задоволення потреб клієнтів відкриває широкі можливості для зловмисників по проведенню атак з таких мереж, що призводить до надмірного використання ресурсів мережі та компроментації її власника. В статті запропоновано структуру ЗКМ, що окрім відомих елементів включає систему виявлення вихідного аномального трафіку. Такий підхід дозволить виявити зловмисників в ЗКМ, зменшити навантаження на мережу та не допускати її компроментації.

Література

1. Real-Time DDoS Attack Detection System Using Big Data Approach. Url: https://doi.org/10.3390/su131910743
2. CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. Url: https://ieeexplore.ieee.org/document/9116932
3. Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. Url: https://ieeexplore.ieee.org/document/9195000
4. Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M., Research of the Neural Network Module for Detecting Anomalies in Network Traffic, CEUR Workshop Proceedingsthis, 2022, 3156, pp. 378–389
5. Звіт за перший квартал 2022 року. Url: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf
6. Звіт за другий квартал 2022 року. Url: https://scpc.gov.ua/api/docs/19b0a96e-8c31-44bf-863e-cd3e0b651f20/19b0a96e-8c31-44bf-863e-cd3e0b651f20.pdf
7. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Url: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#n11
8. Захищені вузли доступу до мережі Інтернет (ЗВІД). Url: https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet
9. Cost of a Data Breach Report 2022. Url: https://www.ibm.com/downloads/cas/3R8N1DZJ
10. У першому кварталі 2022 року DDoS-атаки б'ють рекорди. Url: https://10guards.com/ua/articles/ddos-attacks-at-an-all-time-high-in-q1-2022/
11. State of Phishing & Online Fraud. Url: https://boost.bolster.ai/rs/540-RFH-299/images/2022_PhishingandFraudReport.pdf 6/11/2022

12. Data Breach Investigations Report. Url: https://www.verizon.com/business/resources/T41b/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
13. Перелік категорій кіберінцидентів. Url: https://cert.gov.ua/recommendation/16904 7.11.2022
14. Перший щорічний звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Url: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf
15.What is password cracking? Url: https://www.techtarget.com/searchsecurity/definition/password-cracker
16. Snort. Url: https://www.snort.org/
17. Wireshark Frequently Asked Questions. Url: https://www.wireshark.org/faq.html#_what_is_wireshark
18. Suricata. Url: https://suricata.io/
19. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Url: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7

References

1. Real-Time DDoS Attack Detection System Using Big Data Approach. Url: https://doi.org/10.3390/su131910743
2. CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. Url: https://ieeexplore.ieee.org/document/9116932
3. Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. Url: https://ieeexplore.ieee.org/document/9195000
4. Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M., Research of the Neural Network Module for Detecting Anomalies in Network Traffic, CEUR Workshop Proceedingsthis, 2022, 3156, pp. 378–389
5. Report for the first quarter of 2022. Url: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf
6. Report for the second quarter of 2022. Url: https://scpc.gov.ua/api/docs/19b0a96e-8c31-44bf-863e-cd3e0b651f20/19b0a96e-8c31-44bf-863e-cd3e0b651f20.pdf
7. Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks. Url: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#n11
8. Protected Internet access nodes (PIAN). Url: https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet
9. Cost of a Data Breach Report 2022. Url: https://www.ibm.com/downloads/cas/3R8N1DZJ
10. In the first quarter of 2022, DDoS attacks break records. Url: https://10guards.com/ua/articles/ddos-attacks-at-an-all-time-high-in-q1-2022/
11. State of Phishing & Online Fraud. Url: https://boost.bolster.ai/rs/540-RFH-299/images/2022_PhishingandFraudReport.pdf 6/11/2022
12. Data Breach Investigations Report. Url: https://www.verizon.com/business/resources/T41b/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
13. List of categories of cyber incidents. Url: https://cert.gov.ua/recommendation/16904 7.11.2022
14. The first annual report on the results of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks. Url: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf
15.What is password cracking? Url: https://www.techtarget.com/searchsecurity/definition/password-cracker
16. Snort. Url: https://www.snort.org/
17. Wireshark Frequently Asked Questions. Url: https://www.wireshark.org/faq.html#_what_is_wireshark
18. Suricata. Url: https://suricata.io/
19. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Url: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7