DOI 10.31891/2307-5732-2024-337-3-26
УДК 004.4+336

КОВАЛЕВСЬКИЙ В`ЯЧЕСЛАВ
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0001-7144-1899
e-mail: phd121221_kvv@student.ztu.edu.ua
ВАКАЛЮК ТЕТЯНА
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0001-6825-4697
e-mail: tetianavakaliuk@gmail.com

ОГЛЯД СУЧАСНИХ СИСТЕМ ЗАХИСТУ ЕЛЕКТРОННИХ СЕРВІСІВ

Використання електронних сервісів є невід'ємною частиною сучасного життя. Різноманітні електронні сервіси передають та оброблюють величезні об'єми користувацьких даних. У свою чергу, користувачі електронних сервісів мають бути певними, що всі процеси взаємодії з їх даними відбуваються з дотриманням сучасних безпекових стандартів та не допускають ситуацій отримання несанкціонованого доступу до цих відомостей. У статті проведено огляд наявних сучасних систем захисту, що можуть бути використані для впровадження багаторівневої системи захисту електронних сервісів. Згідно проведеного аналізу, можна побачити, що значну роль у побудові сучасних систем захисту електронних сервісів відіграє впровадження технологій машинного навчання та автоматизація процесів виявлення і попередження загроз. Такий підхід дозволяє значно зменшити час реакції на загрозу, мінімізувати вплив людського фактору та будувати системи захисту, що здатні бути швидко масштабованими в залежності від поставлених задач. Не втрачають свою актуальність і класичні системи забезпечення захисту даних, що опрацьовуються електронними сервісами. До таких можна віднести системи шифрування даних та мережеві брандмауери. Окремо слід відзначити внесок великих технологічних компаній у розвиток безпекової галузі. Надаючи послуги з розміщення електронних сервісів, передачі та обробки даних, технологічні компанії отримують доступ до значної кількості користувацького трафіка, що робить можливим його аналіз для виявлення безпекових ризиків. Окрім цього, ведеться постійна робота над вдосконаленням наявних та розробкою нових систем захисту електронних сервісів з урахуванням сучасних безпекових запитів. Зважаючи на значний вплив впровадження і використання електронних сервісів у глобальній економіці, аналіз економічних наслідків безпекових інцидентів є важливою темою обговорень на міжнародних економічних конференціях як в контексті окремих компаній, так і країн загалом.

Ключові слова: *електронні сервіси, інформаційна безпека, системи захисту, машинне навчання, безпекові загрози.*

KOVALEVSKYI VIACHESLAV, VAKALIUK TETIANA
Zhytomyr Polytechnic State University

REVIEW OF MODERN SYSTEMS FOR THE PROTECTION OF ELECTRONIC SERVICES

The use of electronic services is an integral part of modern life. Various electronic services transmit and process vast volumes of user data. Users of these services must be assured that all interactions with their data are conducted in compliance with modern security standards and prevent unauthorized access. This article reviews the existing modern protection systems that can be implemented to establish a multi-level security system for electronic services. The analysis indicates that machine learning technologies and the automation of threat detection and prevention processes play a significant role in the construction of modern electronic service protection systems. This approach reduces the response time to threats, minimizes the impact of human factors, and enables the construction of security systems that can be quickly scaled depending on the tasks. It is evident that traditional data protection systems, including data encryption systems and network firewalls, retain their relevance in the context of electronic services. Furthermore, the contribution of major technology companies to the security industry should be noted. By providing services for hosting electronic services, data transmission, and processing, these companies gain access to a significant amount of user traffic, enabling them to analyze it for security risks. Additionally, there is ongoing work to improve existing and develop new protection systems for electronic services, taking into account modern security demands. Given the significant impact of the implementation and use of electronic services in the global economy, the economic consequences of security incidents remain a crucial topic of discussion at international economic conferences, both in the context of individual companies and countries as a whole.

Keywords: *electronic services, information security, protection systems, machine learning, security threats.*

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

Забезпечення захисту електронних сервісів являє собою задачу, що ніколи не втрачає своєї актуальності. Постійне зростання кількості електронних сервісів, які є частиною надання різноманітних послуг в сучасному світі, відкриває нові виклики у забезпеченні їх сталого і захищеного функціонування. Розуміння потенційних безпекових загроз та методів їх проактивного усунення являє собою основу побудови комплексів захисту інфраструктури електронних сервісів. Сучасні системи захисту електронних сервісів дозволяють впроваджувати багаторівневий захист, забезпечувати прозоре функціонування та взаємодію електронних сервісів з користувачами.

Аналіз останніх досліджень і публікацій

Проблемі захисту електронних сервісів приділяло увагу багато дослідників, у тому числі Саймон Аппелбаум (Simon Applebaum), Тарек Гейбер (Tarek Gaber), Алі Ахмед (Ali Ahmed), що у своєму дослідженні проводять аналіз роботи брендмауера веб-додатків з використанням машинного навчання [9].

Ito Мічіакі (Ito Michiaki) та Іятомі Хітоші (Iyatomi Hitoshi) досліджували практичний досвід поєднання брандмауера веб-додатків та нейронної мережі [10]. Дослідники Цимін Цао (Qimin Cao), Іньрун Цяо (Yinrong Qiao), Чжун Лю (Zhong Lyu) проводили дослідження використання дворівневого алгоритму машинного навчання для аналізу журналів роботи веб-сервера [15]. Компанія Cloudflare щоквартально публікує аналіз виявлених нею кіберзагроз, інформацію щодо їх усунення та рекомендації для запобігання їх розповсюдженню [11]. Дослідники та безпосередні учасники процесів забезпечення захисту електронних сервісів висвітлюють зазначену проблему враховуючи свій власний досвід та в контексті специфіки своєї професійної діяльності.

Формулювання цілей статті

Метою статті є огляд сучасних систем захисту електронних сервісів, специфіки їх роботи, областей застосування та необхідності впровадження комплексних систем захисту електронних сервісів.

Виклад основного матеріалу

Зважаючи на швидке поширення та розвиток різноманітних електронних сервісів, що зачіпають практично всі сфери життя сучасної людини, слід відзначити постійну увагу до розробки нових і вдосконалення наявних систем захисту електронних сервісів від загроз, що становлять небезпеку як для користувачів електронних сервісів (в контексті втрати персональних даних) так і для їх власників (матеріальні витрати, втрата бізнесу, репутаційні втрати). Сучасні системи захисту електронних сервісів в першу чергу націлені на проактивне запобігання ситуацій, які можуть становити безпекову загрозу, а також мінімізацію наслідків у випадку, коли зловмисники все ж змогли реалізувати свої наміри.

Серед сучасних систем захисту електронних сервісів, що широко використовуються, можна виділити наступні:

- брандмауери (Firewall) та брандмауери веб-додатків (Web Application Firewall (WAF));
- системи виявлення та запобігання вторгненням (IDS\IPS);
- системи моніторингу та журналювання;
- системи шифрування користувацького трафіку та даних.

Слід зазначити, що у більшості випадків ці системи використовуються комплексно, для забезпечення багатошарового захисту від потенційних атак.

Розглянемо ці системи більш детально. Системи виявлення і запобігання вторгненням (IDS/IPS) проводять безперервний моніторинг трафіку, що передається в мережі організації, на предмет підозрілої діяльності (рис.1). Системи IDS і IPS являють собою дві незалежні системи, але у більшості випадків вони використовуються разом, для отримання максимальних результатів їх роботи [1].

Система виявлення вторгнень (IDS) проводить моніторинг трафіку в мережі, аналізує трафік на відповідність сигнатурам відомих атак і, у разі виявлення підозрілої активності, забезпечує інформування відповідальних осіб. Система IDS не перешкоджає атаці, що відбувається [1]. У свою чергу, система запобігання вторгненням (IPS) також проводить моніторинг трафіку мережі, але у випадку виявлення підозрілої активності, трафік блокується та лишається заблокованим до подальшого аналізу ситуації, що склалася і прийняття рішення щодо розблокування [1].

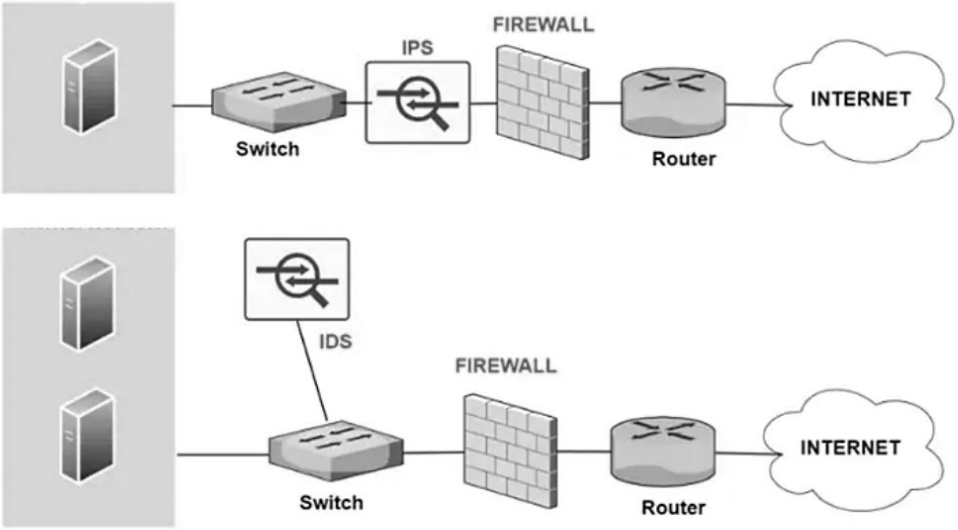

Рис. 1. Діаграма розміщення систем IPS та IDS в мережі [2]

Поєднане впровадження систем виявлення і запобігання вторгненням забезпечує багаторівневий захист мережі, зменшує кількість хибних спрацьовувань, підвищує ефективність управління мережею, що, в свою чергу, сприяє можливості організацій протистояти різноманітним кіберзагрозам.

Брандмауери (Firewall) та брандмауери веб-додатків (Web Application Firewall (WAF)) покликані забезпечувати контроль доступу та захист від несанкціонованого доступу до елементів мережевої

інфраструктури. Маючи спільну мету, вони функціонують на різних рівнях мережевої інфраструктури та зосереджені на різних аспектах безпеки.

Брандмауери – це мережеві безпекові системи задачею яких є контроль вхідного і вихідного трафіку. Брандмауери слугують бар'єром між внутрішньою мережею організації та зовнішнім середовищем. Брандмауер проводить інспекцію вхідних і вихідних пакетів на відповідність заданим правилам проходження трафіку. У разі невідповідності – пакети блокуються [3]. Звичайні брандмауери оперують на мережевому та транспортному рівні моделі OSI, оперуючи трафіком на основі IP адрес та TCP/UDP портів (рис. 2).

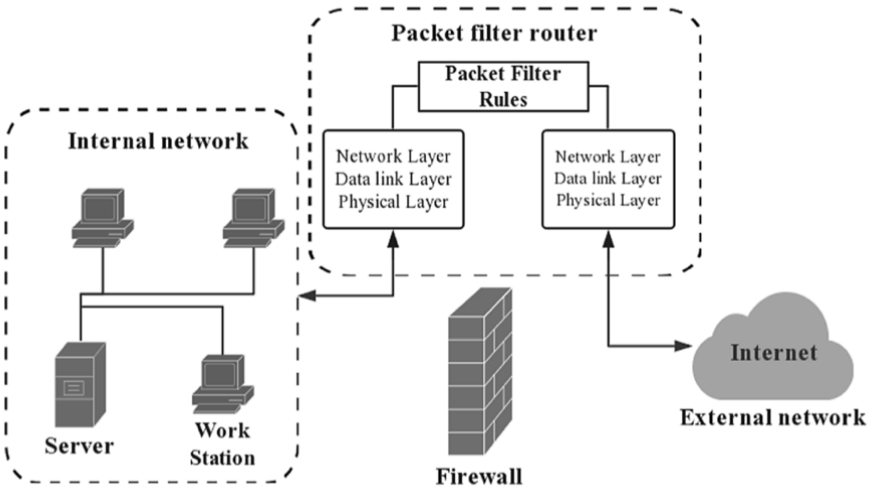

Рис. 2. Мережевий брандмауер [4]

Послідовним етапом розвитку мережевих брандмауерів є Next Generation Firewall (NGFW) – брандмауери наступного покоління, що охоплюють всі можливості традиційних брандмауерів, а також містять інтегровані механізми запобігання вторгнень, можливості контролю трафіку на прикладному рівні, отримують постійні оновлення щодо загальновідомих загроз, мають засоби та можливості для поширення інформації про аномалії для подальшого централізованого аналізу [5].

Розповсюдження і впровадження брандмауерів наступного покоління значно спрощує протидію наявним кіберзагрозам, оскільки обмін інформацією про відомі типи атак відбувається централізовано. У разі виявлення аномалій, що можуть бути індикаторами потенційно небезпечної активності, одним брандмауером, решта, через певний час потрібний для аналізу, отримують інструкції щодо протидії. Це значно пришвидшує реакцію на загрози, та у багатьох випадках запобігає їх подальшому поширенню.

Набір доступного функціоналу серед наявних брандмауерів наступного покоління може відрізнятись залежно від виробника та обраного рівня необхідного захисту. Узагальнені можливості, що можуть бути реалізовані за допомогою NGFW, представлені на рисунку 3.

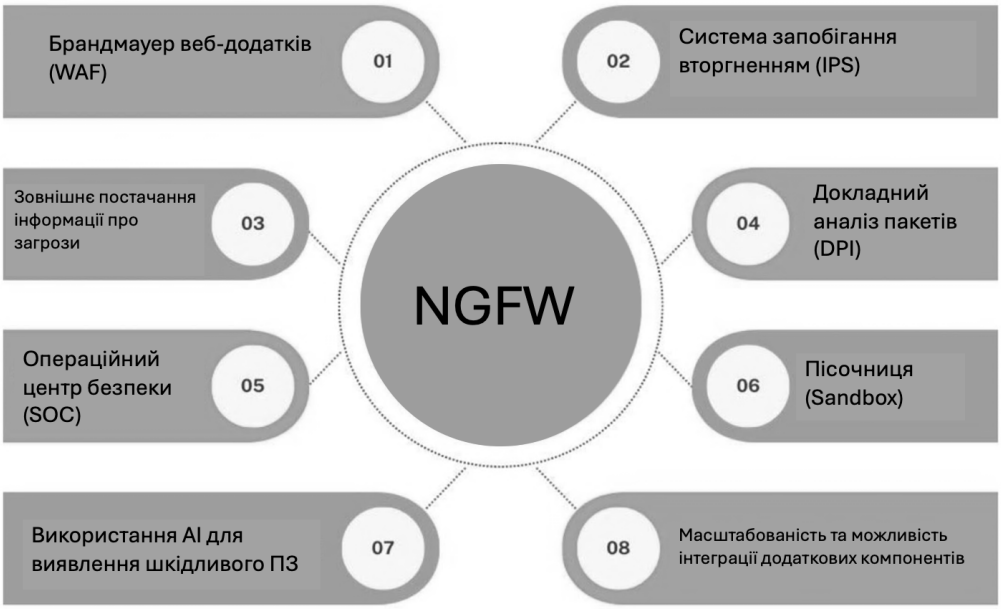

Рис. 3. Ключові можливості NGFW [6]

Незважаючи на широкі можливості брандмауерів наступного покоління, вони мають застосовуватись як частина загальної архітектури безпеки в поєднання з іншими технічними та організаційними заходами. Це дозволяє побудувати цілісну систему запобігання та контролю загроз, що покриває всі безпекові аспекти інформаційної системи [6].

На відміну від звичайних брандмауерів, брандмауери веб-додатків (WAF) є вузькоспеціалізованими засобами забезпечення захисту веб-додатків, що зосереджуються на специфічних для них загрозах. До таких можна віднести SQL ін'єкції (SQL-injections), міжсайтовий скриптинг (XSS), неправомірне використання даних користувацьких сесій та форм, DDoS атаки. Також WAF використовується для захисту API інтерфейсів, захисту від атак мережевих ботів, брутфорс атак [7]. Брандмауери веб-додатків оперують на прикладному рівні моделі OSI.

Брандмауер веб-додатків працює як зворотній проксі (reverse proxy), що убезпечує захищені ресурси від прямої комунікації з користувачами. Всі вхідні запити користувачів проходять через WAF, де проводиться їх аналіз на відповідність заданим політикам і правилам (рис.4). У своїй роботі WAF опирається на використання стратегій позитивної (Positive Security Model) та негативної (Negative Security Model) безпекових моделей [8]. Їх поєднання дозволяє отримати найкращих результатів запобігання загрозам.

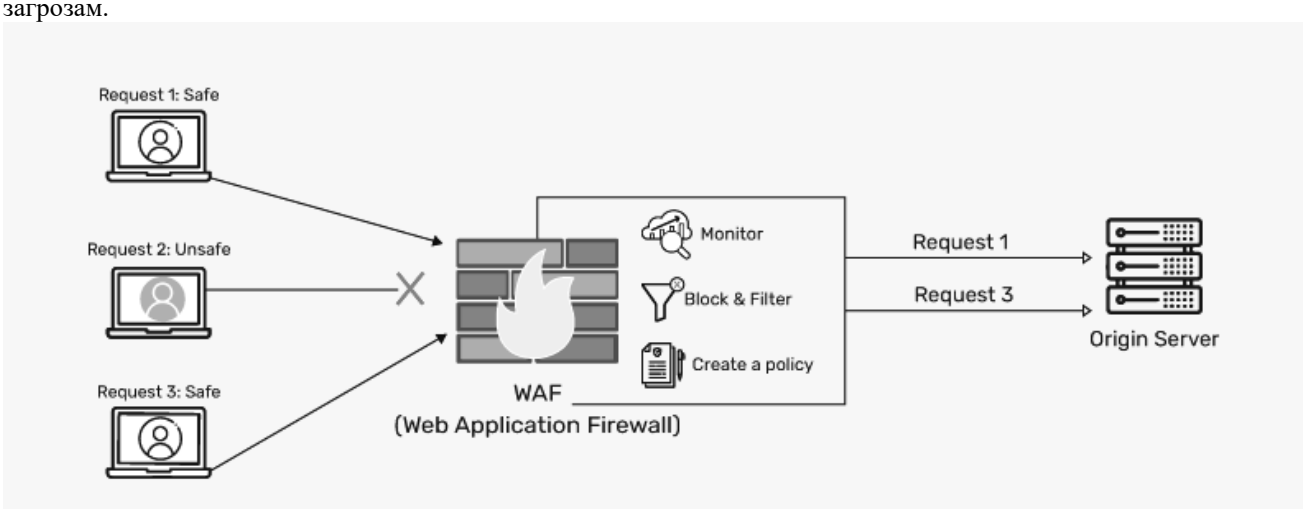

Рис. 4. Брандмауер веб-додатків [8]

Позитивна безпекова модель полягає у чіткому визначенні дозволених шаблонів та поведінки, дозволяючи лише легітимний трафік походження якого відоме та відхиляє все інше, що не збігається зі списком дозволеного [9].

В свою чергу, згідно з негативною безпековою моделлю, відбувається ідентифікація та блокування трафіку, що відповідає відомим шаблонам та сигнатурам, припускаючи, що будь-який трафік, який відповідає попередньо визначеним шаблонам атак є шкідливим [9].

Розвиток технологій штучного інтелекту дозволив значно розширити можливості WAF щодо виявлення та запобігання потенційних загроз. Це досягається шляхом навчання штучного інтелекту на базі атак, що відбуваються та, базуючись на отриманих даних, подальшій адаптації параметрів WAF для більш ефективної роботи [9]. Так дослідники Іто Мічіакі (Ito Michiaki) та Іятомі Хітоші (Iyatomi Hitoshi) використовуючи брандмауер веб-додатків у поєднанні з машинним навчанням змогли досягнути точності 98.8% у виявленні шкідливих запитів, що надходили до тестового середовища [10].

Брандмауери веб-додатків відіграють ключову роль у забезпеченні стабільної роботи різноманітних електронних сервісів. Згідно з даними компанії Cloudflare, що являється одним зі світових лідерів у сфері захисту електронних сервісів, у четвертому кварталі 2023 року спостерігалось зростання загальної кількості DDoS атак на 117% в порівнянні з аналогічним періодом попереднього року (рис. 5) [11]. Використовуючи власні розроблені технології та кооперацію з іншими представниками галузі, компанії Cloudflare вдалося пом'якшити одну з найбільших DDoS атак, що складала 201 мільйон запитів на секунду [11].

Системи моніторингу та журналювання являються невіддільною частиною цілісної архітектури безпеки інформаційної системи. Моніторинг – це можливість мати інформацію, про певний момент у роботі інформаційної системи, а також історичний огляд попередніх станів системи, таких як продуктивність системи, цілісність даних, що обробляються інформаційною системою, доступність компонентів інформаційної системи [12]. Спостереження за цими станами дозволяє створити систему сповіщень, що буде інформувати відповідальних осіб у разі відхилень від заданих значень.

Журналювання – це процес агрегації записів про події, що відбуваються в інформаційній системі [12]. Вагомим фактором успішного впровадження систем журналювання, є визначення корисної інформації для зберігання. Окрім цього, необхідно забезпечити надійне зберігання отриманої інформації, її конфіденційність та проводити періодичні перевірки правильності збору інформації згідно з заданими параметрами.

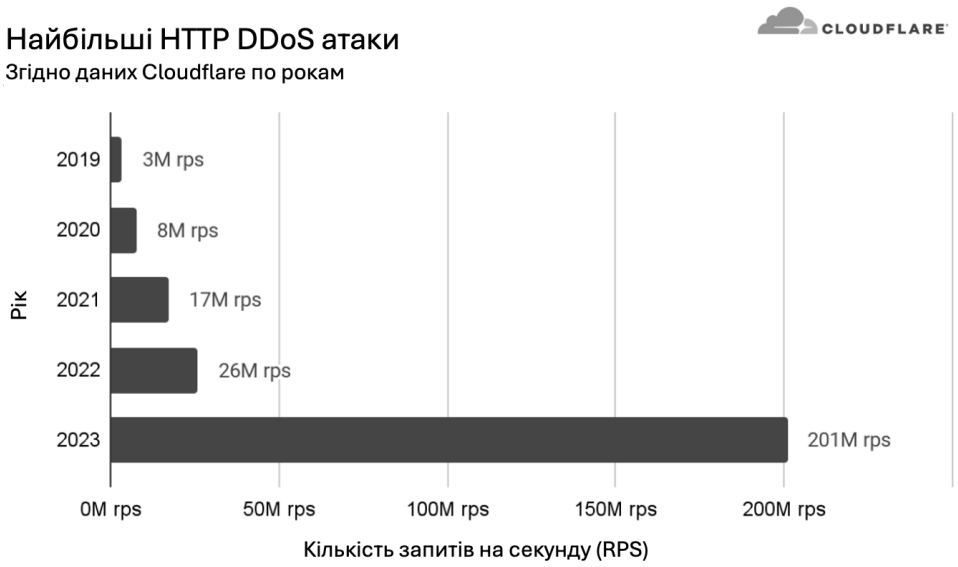

Рис. 5. Найбільші атаки HTTP DDoS за даними Cloudflare [11]

Часто недооцінені, системи моніторингу та журналювання відіграють важливу роль, надаючи можливість вчасно виявляти проблеми та проводити аналіз подій, що відбулися, в розрізі певних проміжків часу. Так організація OWASP, що є визнаним експертом в галузі кібербезпеки, визначає проблеми наявності систем моніторингу та журналювання чи правильності їх налаштування, як одну з десяти найпоширеніших загроз безпеки інформаційних систем [13].

Використання машинного навчання у поєднанні з системами моніторингу та журналювання значно покращує результати аналізу отриманих даних та виявлення аномалій і шаблонних дій, що могли бути непомітними для людини [14]. Як результат, вагомо підвищується швидкість та якість реагування на потенційні загрози, щодо інформаційної системи.

Дослідники Цимін Цао (Qimin Cao), Іньрун Цяо (Yinrong Qiao), Чжун Лю (Zhong Lyu) у своїй роботі описують роботу системи виявлення аномалій з використання машинного навчання для аналізу журналів роботи веб-сервера [15]. Автори пропонують систему виявлення аномалій, яка використовує дворівневий алгоритм машинного навчання (рис.6). Модель дерева рішень класифікує нормальні та аномальні набори даних. Нормальний набір даних вручну перевіряється для створення кількох прихованих марковських моделей (HMM). Експериментальні дані надходили з журналів роботи реального веб-сервера.

Отримані результати показали точність виявлення аномалій на рівні 93.54% та 4.09% хибнопозитивних результатів, в порівнянні з однорівневими алгоритмами машинного навчання. Автори зазначають, будь-яка система виявлення аномалій з використанням машинного навчання, потребує постійного оновлення, оскільки нові атаки змінюються, що в свою чергу знижує ефективність роботи системи виявлення. Тому автори планують додати до запропонованої системи модуль повторного навчання, який має оновлювати застарілі дані системи виявлення автоматично.

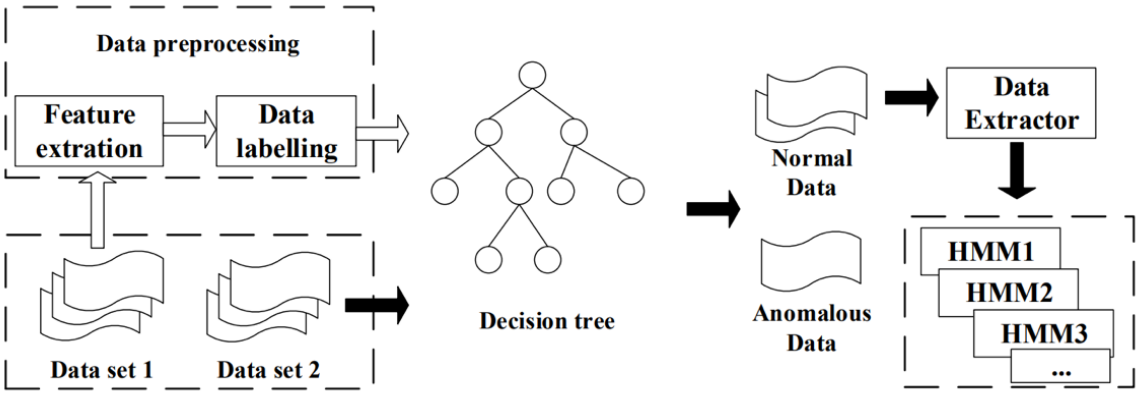

Рис. 6. Діаграма роботи запропонованої системи виявлення аномалій [15]

Системи шифрування користувацького трафіку та даних є однією з основних частин захисту інформаційної системи. Основною метою використання систем шифрування користувацького трафіку та даних є забезпечення цілісності та конфіденційності даних, унеможливлення втручання у процес передачі даних, забезпечення доступності даних для авторизованих користувачів (рис.7) [16].

Рис. 7. Основні вимоги до безпеки мережі та комп'ютерних систем [16]

Одним з найрозповсюдженіших методів захисту користувацького трафіку від стороннього втручання, при роботі з електронними сервісами, є використання захисту на транспортному рівні (TLS). Це криптографічний протокол, що забезпечує безпечну передачу даних з використанням асиметричного шифрування та сертифікатів X.509 [16]. Протокол TLS є оновленою версією SSL, де усунули відомі вразливості. При комунікації з веб-серверами використання TLS реалізовується за допомогою протоколу HTTPS (HTTP, що передається через SSL або TLS). У цьому випадку шифруються наступні елементи комунікації: адреса ресурсу з яким відбувається комунікація, дані що циркулюють між клієнтом і сервером (дані форм, cookies тощо), вміст HTTP заголовків [16].

Також для гарантування безпечної передачі даних, широко використовуються протокол SSH (Secure Shell) та технологія побудови приватних тунелів VPN (Virtual Private Network). Протокол SSH реалізує можливості захищеного доступу до віддалених серверів, обміну файлами та поштовими повідомленнями [16]. В свою чергу технологія VPN дозволяє будувати захищені комунікаційні тунелі між віддаленими вузлами мережі. Дані в такому тунелі передаються у зашифрованому вигляді та повністю виключають зовнішнє втручання при обміні трафіком [17].

Для гарантування цілісності та конфіденційності даних, що зберігаються в середині інформаційної системи, використовуються алгоритми шифрування даних, серед розповсюджених можна виділити такі як AES, Triple DES, RSA, Blowfish, Twofish [18]. Шифрування даних може бути реалізовано як на апаратному рівні, так і на рівні операційної системи, що використовується. Важливо приділити увагу вибору методу шифрування, оскільки при великих об'ємах даних можливі проблеми з продуктивністю інформаційної системи де відбувається робота з зашифрованими даними.

Згідно з доповіддю «Global Cybersecurity Outlook 2024», що була представлена на Всесвітньому економічному форумі, протистояння кіберзагрозам залишається актуальною проблемою для більшості компаній та організацій у всьому світі [19]. Автори доповіді зазначають, що стрімкий розвиток та розповсюдження технологій разом з браком кваліфікованих кадрів у сфері кібербезпеки, є глобальним викликом на шляху до побудови безпечного середовища для функціонування інформаційних систем різних рівнів. Тільки 15% з опитаних організацій зазначили, що володіють необхідними ресурсами, щоб забезпечити значне покращення своєї кібербезпеки у наступні два роки. 52% з опитаних організацій відмічають брак ресурсів та досвідчених спеціалістів для побудови захищених інформаційних систем, які відповідають сучасним вимогам [19].

Серед можливих наслідків кібератак, найбільше занепокоєння опитаних організацій та компаній викликають можливість порушення операційної діяльності, фінансові і репутаційні втрати, втрата доступу до важливих товарів та сервісів (рис.8) [19].

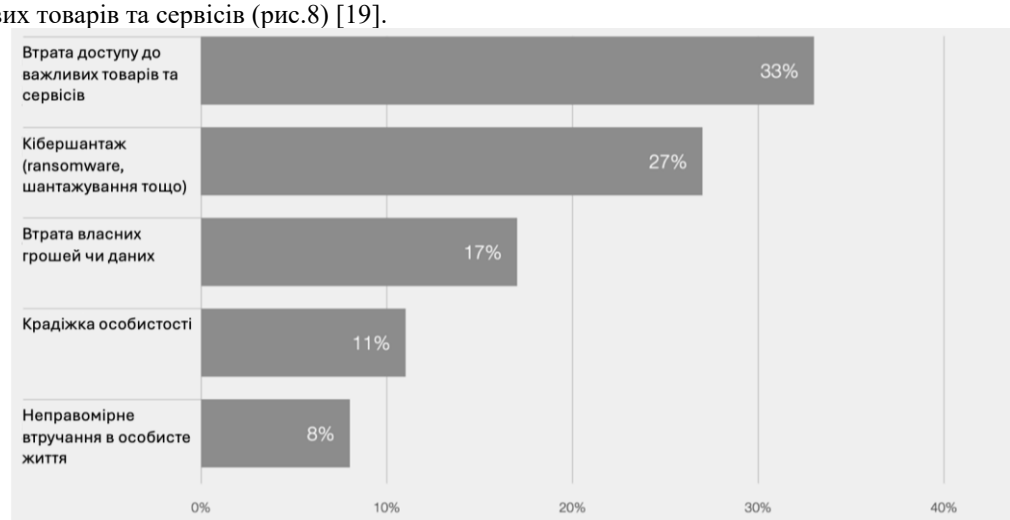

Рис. 8. Найбільші загрози які вбачають опитані організації [19]

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Провівши огляд сучасних систем захисту електронних сервісів можна зробити висновок, що їх розповсюдження та впровадження відіграє важливу роль у побудові цілісного захисту інформаційних систем. Зважаючи на виклики, що стоять перед організаціями, в контексті постійного розширення поля кібератак, нехтування використанням сучасних систем захисту електронних сервісів несе як фінансові, так і репутаційні ризики. Опрацювання інформаційних джерел щодо цієї тематики демонструє постійний розвиток технологій в даній сфері та пошук нових підходів для полегшення інтеграції сучасних систем захисту електронних сервісів з вже працюючими інформаційними системами. Новітні здобутки у сфері використання штучного інтелекту відкривають нові перспективи з вдосконалення наявних та дослідженні і розробці нових технологій і методів забезпечення комплексного захисту електронних сервісів зокрема, та інформаційних систем загалом.

References

1. IDS vs. IPS: definitions, comparisons & why you need both | okta. *Employee and Customer Identity Solutions | Okta*. URL: https://www.okta.com/identity-101/ids-vs-ips/.
2. What is an intrusion detection system? *Palo Alto Networks*. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids.
3. Tanenbaum A. S., Wetherall D. J. Computer networks. Pearson Education, Limited, 2010. 960 p.
4. Securing a network: how effective using firewalls and vpns are? / S. Jingyao et al. *SpringerLink*. URL: https://doi.org/10.1007/978-3-030-12385-7_71.
5. What Is a Next-Generation Firewall (NGFW)? *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html.
6. What is next generation firewall (NGFW)?. *Sangfor Technologies*. URL: https://www.sangfor.com/glossary/cybersecurity/what-is-next-generation-firewall-ngfw.
7. Radware. *DDoS Services: Cloud Security Products and Solutions | Radware*. URL: https://www.radware.com/cyberpedia/application-security/waf-vs-firewall-comparison-and-differences/.
8. How does a WAF (WAAP) work: explained | indusface blog. *Indusface*. URL: https://www.indusface.com/blog/how-web-application-firewall-works/.
9. Applebaum S., Gaber T., Ahmed A. Signature-based and machine-learning-based web application firewalls: a short survey. *Procedia computer science*. 2021. Vol. 189. P. 359–367. URL: https://doi.org/10.1016/j.procs.2021.05.105.
10. Ito M., Iyatomi H. Web application firewall using character-level convolutional neural network. *2018 IEEE 14th international colloquium on signal processing & its applications (CSPA)*, Batu Feringghi, 9–10 March 2018. 2018. URL: https://doi.org/10.1109/cspa.2018.8368694.
11. Yoachimik O., Pacheco J. DDoS threat report for 2023 Q4. *Cloudflare.com*. URL: https://blog.cloudflare.com/ddos-threat-report-2023-q4.
12. Logging & Monitoring: definitions and best practices. *VAADATA - Ethical Hacking Services*. URL: https://www.vaadata.com/blog/logging-monitoring-definitions-and-best-practices/.
13. A09 security logging and monitoring failures - OWASP top 10. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/.
14. Naidu N. Logging and monitoring, the essential holistic view of the systems we build!. *LinkedIn*. URL: https://www.linkedin.com/pulse/logging-monitoring-essential-holistic-view-systems-we-nayan-naidu.
15. Cao Q., Qiao Y., Lyu Z. Machine learning to detect anomalies in web log analysis. *2017 3rd IEEE international conference on computer and communications (ICCC)*, Chengdu, 13–16 December 2017. 2017. URL: https://doi.org/10.1109/compcomm.2017.8322600.
16. Stallings W. Cryptography and network security: principles and practice. Pearson Education, 2020.
17. What is a VPN? How vpns work and why you should use one. *Azure*. URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn.
18. What is data encryption: algorithms, methods and techniques. *Simplilearn.com*. URL: https://www.simplilearn.com/data-encryption-methods-article.
19. Bueermann G., Rohrs M. Global cybersecurity outlook 2024 | INSIGHT REPORT JANUARY 2024. *World Economic Forum*. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.