Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5
DOI: 10.32447/20784643.31.2025.12

Р. Л. Ткачук[1], О. І. Полотай[1], В. С. Балацька[1], Т. Б. Брич[1], Н. П. Кухарська[2]
[1]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
[2]Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID: https://orcid.org/0000-0001-9137-1891 – Р. Л. Ткачук
https://orcid.org/0000-0003-4593-8601 – О. І. Полотай
https://orcid.org/0000-0002-6262-6792 – В. С. Балацька
https://orcid.org/0000-0001-6853-1981 – Т. Б. Брич
https://orcid.org/0000-0002-0896-8361 – Н. П. Кухарська
orest.polotaj@gmail.com

МОДЕЛЮВАННЯ ЗАХИСТУ ОПЕРАЦІЙНИХ СИСТЕМ ВІД РЕАЛІЗАЦІЇ КІБЕРАТАК З ВИКОРИСТАННЯМ КРИТЕРІЮ ПІРСОНА

Постановка проблеми. У сучасних умовах стрімкого розвитку цифрових технологій та зростання кількості кібератак питання ефективного захисту операційних систем набуває особливої актуальності. Традиційні засоби інформаційної безпеки часто не здатні своєчасно реагувати на новітні типи загроз, що постійно еволюціонують та ускладнюються. Однією з ключових проблем залишається недостатня ефективність методів прогнозування кібератак, що не дозволяє своєчасно виявляти потенційні вектори втручання в системи. Водночас, сучасна статистична аналітика відкриває нові можливості для розробки моделей, які здатні визначати ймовірність реалізації атаки ще до її фактичного здійснення. Одним із таких методів є використання коефіцієнта кореляції Пірсона для виявлення закономірностей між системною активністю та ймовірністю кіберінцидентів. Однак на практиці дослідження у цій сфері залишаються фрагментарними, а системний підхід до моделювання захисту з урахуванням статистичних залежностей між параметрами безпеки — недостатньо розроблений. Таким чином, постає проблема розробки комплексної моделі захисту операційних систем від кібератак, яка базується на аналізі кореляційних зв'язків між поведінковими характеристиками системи та ознаками потенційної загрози, з використанням критерію Пірсона як інструменту виявлення значущих залежностей.

Мета. Метою статті є розробка та обґрунтування моделі плану дій захисту операційних систем від кібератак шляхом виявлення кореляційних залежностей між параметрами функціонування системи та індикаторами загроз за допомогою критерію Пірсона, з подальшим застосуванням отриманих результатів для прогнозування ймовірності реалізації атак та вдосконалення систем виявлення аномалій у кіберпросторі.

Результати. У статті представлено результати дослідження, спрямованого на моделювання захисту операційних систем від кібератак із використанням критерію Пірсона як інструменту для виявлення статистично значущих зв'язків між кількісними випадками реалізації кіберзагроз щодо операційних систем різних типів. На основі отриманих результатів змодельовано план заходів із кібербезпеки для операційних систем Windows і Linux з урахуванням їх специфіки та рівнозначної вразливості до кібератак. Описано ключові напрями захисту, включно з оновленням систем, контролем доступу, моніторингом, мережевою безпекою, резервуванням та навчанням персоналу.

Висновки. Запропоноване моделювання на основі критерію Пірсона дозволяє ефективно виявляти статистичні закономірності, що передують кібератакам на операційні системи. Застосування такого підходу підвищує рівень превентивного захисту та сприяє своєчасному виявленню потенційних загроз.

Ключові слова: операційна система, кібератака, моделювання, кібербезпека, критерій Пірсона.

R. L. Tkachuk[1], O. I. Polotai[1], V. S. Balatska[1], T. B. Brych[1], N. P. Kukharska[2]
[1]*Lviv State University of Life Safety, Lviv, Ukraine*
[2]*Lviv Polytechnic National University, Lviv, Ukraine*

MODELING THE PROTECTION OF OPERATING SYSTEMS FROM CYBERATTACKS USING THE PEARSON CRITERION

Introduction. In today's conditions of rapid development of digital technologies and the increase in the number of cyberattacks, the issue of effective protection of operating systems is becoming particularly relevant. Traditional information security tools are often unable to respond in a timely manner to the latest types of threats that are constantly evolving and becoming more complex. One of the key problems remains the insufficient effectiveness of methods for predicting cyberattacks, which does not allow for timely detection of potential vectors of interference in systems. At the same time, modern statistical analytics opens up new opportunities for developing models that can determine the probability of an attack even before it is actually carried out. One of such methods is the use of the Pearson correlation coefficient to identify patterns between system activity and the probability of cyber incidents. However, in practice, research in this area remains fragmented, and a systematic approach to modeling protection - taking into account statistical dependencies between security parameters - is still developed. Thus, the arises a need to develop a comprehensive model for protecting operating systems from cyberattacks. This model should be based on the analysis of correlations between the system's behavioral characteristics and indicators of a potential threat, using the Pearson criterion as a tool for identifying significant dependencies.

Purpose. The purpose of this article is to develop and substantiate a model of an action plan for protecting operating systems from cyberattacks. The proposed model identifies correlations between system performance parameters and threat indicators using the Pearson criterion, and applies the results to predict the probability of attacks and enhance anomaly detection systems in cyberspace.

Results. The article presents the results of a study that modelled the protection of operating systems against cyberattacks. The study used the Pearson criterion to identify statistically significant relationships between quantitative cyberthreat cases against different types of operating system.

A cybersecurity action plan for Windows and Linux operating systems was modelled based on the results obtained, taking into account their specifics and equivalent vulnerability to cyberattacks.

The key areas of protection are outlined, including system updates, access control, monitoring, network security, redundancy and staff training.

Conclusion. The proposed modelling, based on the Pearson criterion, enables the effective detection of statistical patterns preceding the implementation of cyberattacks on operating systems.

The use of such an approach increases the level of preventive protection and contributes to the timely detection of potential threats.

Keywords: operating system, cyberattack, modeling, cybersecurity, Pearson criterion.

Вступ. У контексті швидкого розвитку технологій дедалі актуальнішим стає питання забезпечення надійного захисту операційних систем від різноманітних кібератак. З кожним роком зловмисники розробляють нові методи впливу на електронні пристрої та інформаційні системи, які зберігають цінні дані. Для ефективної протидії таким загрозам необхідно постійно вдосконалювати стратегії захисту й тестування систем. Один із дієвих методів полягає в імітації кібератак на власну операційну систему з подальшим аналізом отриманих результатів. Такі дані доцільно порівнювати з метою виявлення статистичних закономірностей, що дозволяє робити обґрунтовані висновки та приймати ефективні рішення щодо зміцнення кіберзахисту.

У 2024 році Державна служба спеціального зв'язку та захисту інформації України зафіксувала та опрацювала 1042 кіберінциденти, з яких більше половини – 58,8% – становили випадки, пов'язані із застосуванням шкідливого програмного забезпечення. Така статистика свідчить про збереження високої активності зловмисників у сфері кібератак і актуальність проблеми захисту інформаційних систем.

Питаннями дослідження критерію Пірсона займалися ряд вітчизняних вчених, серед яких Моцний Ф. [10,11], Петрова М. [12], Сальнікова С. [14], Карташов М., Куц В., Лисенко Ю. Однак з огляду на обмежену кількість наукових праць, які присвячені дослідженню вразливостей операційних систем сімейства Windows та Linux з використанням цього методу, застосування критерію Пірсона є новим, перспективним напрямом дослідження.

Методи досліджень. Методологічна база дослідження ґрунтується на принципах діалектичного підходу до пізнання соціальних явищ і процесів, а також на розумінні розвитку й взаємозв'язків об'єктів реальної дійсності. Вона включає систему загальнонаукових і спеціальних методів, що використовуються як інструменти наукового аналізу в гуманітарних науках, зокрема в юриспруденції.

Результати досліджень. Особливості реалізації кібератак на операційні системи можна

згрупувати за певними спільними ознаками. Заслуговують на увагу такі:

Масштабність та автоматизація атак

Сучасні кібератаки часто реалізуються за допомогою автоматизованих засобів, що дає змогу зловмисникам охоплювати велику кількість цілей одночасно. Показовим прикладом є атака програмою-вимагачем WannaCry, яка у травні 2017 року вразила приблизно 200000 комп'ютерів у 150 країнах. Вона експлуатувала вразливість в операційній системі Windows, що дозволило шкідливому ПЗ швидко поширюватися через мережу без потреби у взаємодії з користувачем.

Експлуатація вразливостей у програмному забезпеченні

Зловмисники постійно вишукують і використовують вразливості в операційних системах з метою отримання несанкціонованого доступу або запуску шкідливого програмного забезпечення. Яскравим свідченням критичної важливості контролю якості оновлень стало масове порушення роботи близько 8,5 мільйонів систем Windows у липні 2024 року, спричинене помилковим оновленням безпеки від компанії CrowdStrike. Цей інцидент наголосив на необхідності ретельного тестування та перевірки змін перед їх масштабним розгортанням.

Цілеспрямовані атаки на критичну інфраструктуру

Операційні системи, що забезпечують функціонування об'єктів критичної інфраструктури — зокрема в галузях енергетики, охорони здоров'я та державного управління — є особливо привабливими цілями для цілеспрямованих кібератак. У 2024 році в Україні було зафіксовано 4315 кіберінцидентів, що на 69,8% більше порівняно з попереднім роком. Основними об'єктами атак залишались урядові установи, енергетичні підприємства та телекомунікаційні компанії, що підкреслює високий рівень ризику для життєво важливих цифрових систем.

Використання шкідливого програмного забезпечення

Програми-вимагачі залишаються однією з найпоширеніших загроз для операційних систем. Згідно зі звітом Elastic Global Threat Report 2023, сімейства програм-вимагачів BlackCat, Conti, Hive, Sodinokibi та Stop відповідальні за приблизно 81% усієї активності програм-вимагачів.

Одним із способів визначення статистичних залежностей між двома вибірками у непараметричній статистиці є застосування коефіцієнта погодженості Пірсона χ^2.

Коефіцієнт погодженості Пірсона χ^2 (критерій χ^2 (хі-квадрат)) – коефіцієнт, що ґрунтується на наближенні частоти прояву ознаки у різних вибірках, виміряної за номінативною шкалою. Його використовують для порівняння частот двох розподілів: двох емпіричних або емпіричного і теоретичного

Актуальність використання критерію Пірсона зумовлена необхідністю виявлення прихованих зв'язків між параметрами інформаційної системи (такими як зміни в мережевому трафіку, кількість несанкціонованих запитів, аномальна активність користувачів) та фактом здійснення кібератаки. Завдяки цьому методу можна оцінити кореляцію між поведінковими ознаками системи та подіями безпеки, що дозволяє будувати моделі раннього запобігання. Застосування критерію Пірсона у поєднанні з інструментами машинного навчання дозволяє значно підвищити точність прогнозування та знизити ризики несанкціонованого втручання.

Розрахунок здійснюють за формулою:

$$\chi 2 = \frac{\sum(n_{i1}-n_{i2})^2}{n_{i2}} \quad (1)$$

де n_{i1} – частота P^1 прояву властивості у першого досліджуваного; n_{i2} – частота P^2 прояву властивості у другого досліджуваного.

Застосування критерію вимагає, щоб обсяг розподілів, що зіставляються, мав не менше 20-30 варіантів, а мінімальна їх частота – не менше п'яти (інакше слід укрупнити розряди).

Щоб краще зрозуміти застосування критерію Пірсона для прогнозування кібератак на операційні системи, розглянемо приклад: ми досліджуємо системну активність за останні пів року та встановлюємо, що коефіцієнт кореляції Пірсона між кількістю невдалих спроб входу та випадками несанкціонованого доступу становить r = 0,82. Такий показник свідчить про наявність сильної позитивної залежності — зі зростанням кількості невдалих входів підвищується ймовірність атаки. Отже, подібний показник слід обов'язково враховувати в системах автоматизованого виявлення загроз.

Коефіцієнт Пірсона використовується для порівняння частот у двох розподілах — як між двома емпіричними, так і між емпіричним і теоретичним. Його основна суть полягає в зіставленні емпіричної таблиці двовимірного розподілу з теоретичною таблицею тієї ж структури (з однаковою кількістю рядків і стовпців), яка моделює ситуацію повної статистичної незалежності між ознаками [14]. Для коректного застосування критерію необхідно, щоб загальна кількість варіантів у розподілах становила не менше 20–30, а найменша частота в таблиці – не менше п'яти.

$$\chi 2 = \sum \frac{(f_i' - f_i'')^2}{f_i' + f_i''} \quad (2)$$

де f_i' і f_i'' – частоти двох вибірок, що зіставляються. Отриману суму порівнюють з табличним

значенням того або іншого рівня значущості. Застосування критерію вимагає, щоб обсяг розподілів, що зіставляються, мав не менше 20-30 варіантів, а мінімальна їх частота – не менше п'яти.

Алгоритм обчислення вказаного коефіцієнта можна з'ясувати на прикладі. При виявленні реалізації кіберзагрози у двох типах операційних систем експериментальним чином отримано результати випадків одночасної реалізації різних видів загроз, розміщені в таблиці 1.

Таблиця 1

Результати кількості одночасної реалізації різних видів кіберзагроз

Обсяг одночасного виявлення кіберзагрози	Кількість досліджуваних кіберзагроз з першої операційної системи сімейства Windows	Кількість досліджуваних кіберзагроз з другої операційної системи сімейства Linux	Обсяг одночасного виявлення кіберзагрози	Кількість досліджуваних кіберзагроз з першої операційної системи сімейства Windows	Кількість досліджуваних кіберзагроз з другої операційної системи сімейства Linux
x_i	f_i'	f_i''	x_i	f_i'	f_i''
2	4	4	27	5	7
3	7	9	28	7	6
4	8	12	29	8	8
5	12	7	30	9	8
6	9	8	31	10	7
7	9	8	32	7	7
8	12	10	33	8	7
9	10	11	34	8	7
10	10	10	35	8	7
11	9	9	36	9	8
12	11	10	37	10	9
13	15	12	38	11	12
14	14	11	39	8	7
15	13	10	40	7	8
16	8	8	41	6	5
17	8	6	42	9	7
18	7	7	43	12	9
19	10	8	44	12	9
20	11	9	45	11	8
21	15	12	50	8	7
22	18	11	60	7	6
23	11	9	70	7	6
24	8	9	80	6	5
25	7	10	90	5	8
26	8	6	100	3	6

Слід з'ясувати, чи значущою є відмінність частот у цих двох групах. Кількість складених розрядів f = 50.

Обчислення χ^2 наведено в табл. 2, використовуючи формулу 1.

Таблиця 2

Обчислення коефіцієнта погодженості

x_i	f_i'	f_i''	$f_i' - f_i''$	$(f_i' - f_i'')^2$	$f_i' + f_i''$	$\frac{(f_i' - f_i'')^2}{f_i' + f_i''}$
2	4	4	0	0	8	0
3	7	9	-2	4	16	0,25
4	8	12	-4	16	20	0,8
5	12	7	5	25	19	1,315789
6	9	8	1	1	17	0,058824
7	9	8	1	1	17	0,058824
8	12	10	2	4	22	0,181818
9	10	11	-1	1	21	0,047619

Продовження таблиці 2

x_i	f_i'	f_i''	$f_i' - f_i''$	$(f_i' - f_i'')^2$	$f_i' + f_i''$	$\frac{(f_i' - f_i'')^2}{f_i' + f_i''}$
10	10	10	0	0	20	0
11	9	9	0	0	18	0
12	11	10	1	1	21	0,047619
13	15	12	3	9	27	0,333333
14	14	11	3	9	25	0,36
15	13	10	3	9	23	0,391304
16	8	8	0	0	16	0
17	8	6	2	4	14	0,285714
18	7	7	0	0	14	0
19	10	8	2	4	18	0,222222
20	11	9	2	4	20	0,2
21	15	12	3	9	27	0,333333
22	18	11	7	49	29	1,689655
23	11	9	2	4	20	0,2
24	8	9	-1	1	17	0,058824
25	7	10	-3	9	17	0,529412
26	8	6	2	4	14	0,285714
27	5	7	-2	4	12	0,333333
28	7	6	1	1	13	0,076923
29	8	8	0	0	16	0
30	9	8	1	1	17	0,058824
31	10	7	3	9	17	0,529412
32	7	7	0	0	14	0
33	8	7	1	1	15	0,066667
34	8	7	1	1	15	0,066667
35	8	7	1	1	15	0,066667
36	9	8	1	1	17	0,058824
37	10	9	1	1	19	0,052632
38	11	12	-1	1	23	0,043478
39	8	7	1	1	15	0,066667
40	7	8	-1	1	15	0,066667
41	6	5	1	1	11	0,090909
42	9	7	2	4	16	0,25
43	12	9	3	9	21	0,428571
44	12	9	3	9	21	0,428571
45	11	8	3	9	19	0,473684
50	8	7	1	1	15	0,066667
60	7	6	1	1	13	0,076923
70	7	6	1	1	13	0,076923
80	6	5	1	1	11	0,090909
90	5	8	-3	9	13	0,692308
100	3	6	-3	9	9	1
						Σ=12,81 χ^2=12,81

Щоб зробити висновок про прийняття або відхилення гіпотези щодо подібності характеристик різних операційних систем у контексті реалізації кібератак, застосовується табличне значення критерію Пірсона. Його порівнюють із обчисленим значенням цього критерію. Для виконання такого порівняння необхідно визначити кількість ступенів свободи k, яка розраховується як кількість порівнюваних розрядів f, зменшена на одиницю. У нашому прикладі це к = f – 1 = 50 – 1 = 49.

Оскільки табличне значення $\chi_{0,5}(49)=66,351$ [12] і обчислене емпіричне $12,81< \chi_{0,5}$ означає відсутність відмінностей між частотами у двох типах досліджуваних операційних систем, то обидві емпіричні сукупності можна вважати вибірками з однієї генеральної сукупності. Це означає, що досліджувані операційні системи мають приблизно однакові властивості організації інформаційної безпеки, демонструють подібний рівень організації інформаційної безпеки і їх

можна аналізувати в межах однієї моделі. Відповідно можна зробити такі висновки:

Рівнозначний рівень захисту свідчить про те, що незалежно від обраної операційної системи користувачі мають подібний ступінь захищеності від кіберзагроз. Це також може означати, що системи дотримуються спільних принципів безпеки — наприклад, схожих підходів до реалізації контролю доступу, шифрування або управління оновленнями. Водночас, однаковий рівень захисту може свідчити й про подібні вразливості: типові ризики та слабкі місця повторюються, тому потребують уніфікованих або координаційних підходів до побудови стратегії кіберзахисту.

Одним із ключових завдань у сфері кібербезпеки є здатність не лише фіксувати факти кіберінцидентів, але й прогнозувати ймовірність їх виникнення. Для цього широко використовуються методи статистичного аналізу, зокрема критерій Пірсона — коефіцієнт лінійної кореляції, який дозволяє виявити силу та напрямок зв'язку між двома кількісними змінними.

Оскільки обидві операційні системи демонструють подібні характеристики з точки зору кібербезпеки, можна припустити, що за умов однакового навантаження чи за наявності ідентичних векторів атаки (фішингові кампанії або використання відомих вразливостей), ймовірність успішної реалізації кібератаки буде приблизно однаковою. Таким чином, у разі появи вразливості в одній системі — наприклад, відкритого порту чи використання застарілого програмного забезпечення – інша система також може опинитися під загрозою за аналогічних умов, якщо не застосовані додаткові заходи безпеки.

У контексті моделювання кібератак на операційні системи критерій Пірсона може бути застосований для аналізу залежностей між різними параметрами функціонування інформаційних систем та ймовірністю настання інцидентів безпеки. Наприклад, можна дослідити, як зміна кількості підозрілих запитів, частота доступу до певних служб або зміни в поведінці користувачів корелюють з випадками несанкціонованого доступу або активації шкідливого програмного забезпечення.

В результаті отриманих даних, виникла можливість моделювання майбутньої ситуації. Припустімо, що дві організації використовують різні типи операційних систем (наприклад, операційна система першого типу – Windows Server, система другого типу – Linux Ubuntu Server). Обидві операційні системи мають однакову політику доступу, відкриті порти 22 (SSH), 80 (HTTP) і 443 (HTTPS).

У системі виявлено зростання кількості спроб автентифікації з підозрілих IP-адрес – до 2000 за добу. Журнали подій (системи логування) обох операційних систем демонструють підвищену активність сканування портів і спроб експлуатації вразливості CVE-2024-XXXX.

Через брутфорс-атаку зловмисник отримує доступ до облікового запису з недостатньо надійним паролем. У результаті компрометації встановлюється бекдор, через який виконується витік даних або розгортання програм-вимагачів.

Оскільки обидві операційні системи мають схожі властивості захисту, атака реалізується з подібною динамікою.

Як наслідок, відбувається таке:

– порушення цілісності лог-файлів;

– компрометація облікових записів адміністраторів;

– витік критичної інформації;

– необхідність повного аудиту та відновлення системи.

Якщо два типи операційних систем мають однакові властивості до кібератак, це свідчить про рівнозначну вразливість і потребу в однаково ретельному захисті. У такій ситуації важливо впроваджувати проактивні заходи безпеки (двофакторна автентифікація, сегментація мережі, моніторинг активності в реальному часі). Навіть якщо системи демонструють схожі характеристики, будь-яка з них може стати жертвою атаки за умов недостатньої реакції на попереджувальні ознаки загроз.

Виходячи з цього, доцільним є запровадження плану дій із забезпечення кібербезпеки для обох типів операційних систем, який представлений в таблиці 3.

Таблиця 3

Шляхи забезпечення кібербезпеки операційних систем різних типів

Дія	Кроки
Оцінка ризиків та інвентаризація	Визначити всі пристрої, на яких встановлені операційні системи
	Провести аудит наявного програмного забезпечення та відкритих портів
	Оцінити критичність кожного активу
Оновлення та патч-менеджмент	Налаштувати автоматичне оновлення операційних систем та програм
	Регулярно перевіряти наявність безпекових патчів
	Забезпечити тестування оновлень перед впровадженням у виробниче середовище.

Продовження таблиці 3

Захист доступу	Впровадити багатофакторну автентифікацію
	Обмежити доступ до систем за принципом найменших привілеїв
	Використовувати безпечні політики паролів
Мережевий захист	Налаштувати фаєрволи та IDS/IPS
	Впровадити VPN для віддаленого доступу
	Сегментувати мережу для обмеження поширення загроз
Моніторинг та логування	Вести централізоване логування дій користувачів і систем
	Аналізувати логи на предмет аномальної активності
	Використовувати SIEM-системи для автоматичного виявлення інцидентів
Резервне копіювання	Налаштувати регулярне резервне копіювання важливих даних
	Зберігати копії в ізольованих середовищах
	Регулярно тестувати процес відновлення
Навчання персоналу	Проводити регулярні тренінги з безпеки
	Навчати користувачів розпізнавати фішингові атаки та інші загрози
	Розробити політику реагування на інциденти
Інцидент-респонс	Створити чіткий план реагування на інциденти
	Визначити відповідальних осіб
	Проводити навчання на симульованих загрозах

Якщо моделювати план дій із кібербезпеки, відштовхуючись від конкретної операційної системи, окремо для Windows та Linux, з урахуванням їх специфіки, то можна запропонувати заходи, які представлені в таблиці 4.

Таблиця 4

Шляхи забезпечення кібербезпеки операційних систем різних типів

Операційна система	Дія	Пояснення
Windows	Оцінка та оновлення	Використання Windows Update та WSUS для централізованого оновлення
		Видалення застарілих компонентів (наприклад, Internet Explorer)
	Захист доступу	Увімкнення BitLocker для шифрування дисків
		Використання Active Directory з політиками групової безпеки (GPO).
	Мережевий захист	Налаштування Windows Firewall з розмежуванням по профілях
		Увімкнення Windows Defender Advanced Threat Protection (ATP)
	Моніторинг	Використання Event Viewer, Sysmon, та Microsoft Sentinel для збору логів
		Активація аудиту входів, запуску програм і змін системних файлів
	Навчання та резервування	Впровадження політик «найменшого привілею» для користувачів
		Використання Windows Backup або Veeam для резервного копіювання
Linux	Оцінка та оновлення	Регулярні оновлення через apt, yum, або dnf
		Видалення непотрібних служб (наприклад, Telnet, FTP)
	Захист доступу	Вимкнення root-доступу по SSH
		Використання sudo з обмеженими правами
		Впровадження SELinux або AppArmor
	Мережевий захист	Налаштування iptables або nftables
		Встановлення Fail2Ban для захисту від брутфорсу
	Моніторинг	Використання журналів syslog, auditd, logwatch
		Розгортання систем типу OSSEC або Wazuh для аналізу безпеки
		Навчання та резервування
		Регулярна перевірка прав доступу (chmod, chown)
	Резервне копіювання	Резервне копіювання за допомогою rsync, Borg, або Duplicity

Висновки. Кібератаки на операційні системи залишаються однією з найсерйозніших загроз у сфері кібербезпеки, особливо в умовах зростаючої цифровізації та геополітичної нестабільності. Операційні системи, як основа функціонування комп'ютерних систем, є привабливою ціллю для зловмисників через їхню критичну роль у забезпеченні роботи інфраструктури та обробці конфіденційних даних.

Таким чином, дослідження використання статистичних методів, зокрема критерію Пірсона, в контексті прогнозування кібератак є важливим кроком у створенні більш безпечного цифрового середовища як для державних установ, так і для приватного сектору.

Кібератаки на операційні системи стають все більш складними та масштабними, що вимагає від організацій постійного вдосконалення заходів кібербезпеки. Особливу увагу слід приділяти своєчасному оновленню систем, впровадженню багатофакторної автентифікації, моніторингу мережевої активності та навчанню персоналу основам кібергігієни.

Список літератури:

1. F.H.Y. Bhaiji, Network security technologies and solutions. Indianapolis, IN, USA: Cisco Press, 2008, ISBN: 978-1-58705-246-0]
2. Kachold Lisa. Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators // Linuxgazette.net, July 2009 (# 164)
3. Snedecor G.W., Cochran W. G. Statistical methods. 6th ed. Iowa: Iowa State University Press, 1967. 593 p.
4. Балацька В.С., Полотай О.І., Брич Т.Б. Особливості потреб у захисті операційних систем. V Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів «*Інформаційна безпека та інформаційні технології*». Львів, ЛДУБЖД, 30 листопада 2022 р. С. 286–288.
5. Безпека у Windows [Електронний ресурс] – Режим доступу до ресурсу: support. microsoft.com
6. Бєляєва Д.В. Економіко-математичне моделювання у дослідженнях економічних систем Матеріали XV Всеукраїнської науково-практичної конференції «*Моделювання та прогнозування економічних процесів*». К, 2021. С. 9-10.
7. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. *Наукоємні технології*, 2012. № 3 (15)
8. Кучернюк П.В. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). *Мікросистеми, Електроніка та Акустика* : науково-технічний журнал. – 2017. – Т. 22, № 6(101). – С. 64–70.
9. Моцний Ф.В. Аналіз непараметричних і параметричних критеріїв перевірки статистичних гіпотез. Частина І. Критерії узгодження Пірсона і Колмогорова. СТАТИСТИКА УКРАЇНИ, 2018, № 4, С. 14-24.
10. Моцний Ф.В. Статистичні розподіли хі-квадрат, Стьюдента, Фішера – Снедекора та їх застосування // *Статистика України*. 2018. № 31 (80). С. 16–23.
11. Моцний Ф.В. Сучасний базовий інструментарій математичної статистики. Ч. I, II // *Науковий вісник НАСОА*. 2015. № 2, С. 16–29. № 3, С. 14–25.
12. Петрова М.А. Таблиці критичних значень основних статистичних критеріїв. Методична розробка для практичних занять з дисципліни «Основи статистичного обліку в екології» для курсантів та студентів напряму підготовки 6.040106 «Екологія, охорона навколишнього середовища та збалансоване природокористування», Львів, 2012. – 10 с.
13. Полотай О.І. Порівняння особливостей операційних систем через призму реалізації кібератак за допомогою критерію Пірсона. Міжнародна мультидисциплінарна наукова інтернет-конференція "*Світ наукових досліджень*". Тернопіль, Україна, м. Ополе, Польща, 25-26 березня 2025 р. Вип. 39. С. 199-202.
14. Сальнікова С. Застосування критерію Пірсона до визначення структури тестових завдань. Соціологічні студії. 2015. № 1. С. 78-83.
15. Трофименко О.Г., Дубовой Я.В. Щодо правового потенціалу безпечного функціонування кіберпростору. *Кібербезпека в Україні: правові та організаційні питання*: матер. III всеукраїнської наук.-практ. конф. (м. Одеса 30 листопада 2018 р.). Одеса: ОДУВС. С. 5–7.

References:

1. F.H.Y. Bhaiji, Network security technologies and solutions. Indianapolis, IN, USA: Cisco Press, 2008, ISBN: 978-1-58705-246-0]
2. Kachold Lisa. Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators // Linuxgazette.net, July 2009 (# 164)
3. Snedecor G.W., Cochran W. G. Statistical methods. 6th ed. Iowa: Iowa State University Press, 1967. 593 p.
4. Balatska V.S., Polotai O.I., Brych T.B. (2022). Osoblivosti potreb u zakhisti operatsiinikh sistem. "*Informatsiina bezpeka ta informatsiini tekhnologii*" [Information Security and Information Technologies in All-Ukrainian Scientific-Practical Conference of Young Scientists, Students and Cadets] (pp. 286–288). November 30, 2022, Lviv, Ukraine [in Ukrainian]
5. Bezpeka u Windows. [Security in Windows]. [URL]: https://support.microsoft.com
6. Bєlyaєva D.V. (2021). Economic and mathematical modeling in economic systems research. In *Modelyuvannya ta prognozuvannya yekonomichnikh protsesiv* [Modeling and forecasting of economic processes in XV All-Ukrainian

Scientific and Practical Conference] (pp. 9-10). [in Ukrainian]

7. Kornienko B.Ya. (2012). Doslidzhennya modeli vzaєmodiї vidkritikh sistem z poglyadu informatsiinoї bezpeki. [Research on the model of interaction of open systems from the point of view of information security]. Naukoємni tekhnologiї – Scientific technologies. [in Ukrainian]

8. Kuchernyuk P.V. (2017). Metodi i tekhnologiї zakhistu komp'yuternikh merezh (fizichnii ta kanalnii rivni). [Methods and technologies for protecting computer networks (physical and link levels)]. Mikrosistemi, Yelektronika ta Akustika - Microsystems, Electronics and Acoustics. 64–70. [in Ukrainian]

9. Mocnyj F.V. (2018). Analiz neparametrichnikh i parametrichnikh kriteriїv perevirki statistichnikh gipotez. Chastina I. Kriteriї uzgodzhennya Pirsona i Kolmogorova. [Analysis of nonparametric and parametric criteria for testing statistical hypotheses. Part I. Pearson and Kolmogorov agreement criteria]. Statistika Ukraïni - Statistics of Ukraine. 14-24. [in Ukrainian]

10. Mocnyj F.V. (2018). Statistichni rozpodili khi-kvadrat, Styudenta, Fishera – Snedekora ta їkh zastosuvannya. [Chi-square, Student, Fisher-Snedecor statistical distributions and their applications]. Statistika Ukraïni - Statistics of Ukraine. 16–23. [in Ukrainian]

11. Mocnyj F.V. (2015). Suchasnii bazovii instrumentarii matematichnoї statistiki. [Modern basic tools of mathematical statistics]. Naukovii visnik NASOA - NASA Science Bulletin. 14–25. [in Ukrainian]

12. Petrova M.A. (2012). Tablitsi kritichnikh znachen osnovnikh statistichnikh kriteriїv. Metodichna rozrobka dlya praktichnikh zanyat z distsiplini «Osnovi statistichnogo obliku v yekologiї» dlya kursantiv ta studentiv napryamu pidgotovki 6.040106 «Ekologiya, okhorona navkolishnogo seredovishcha ta zbalansovane prirodokoristuvannya». [Tables of critical values of the main statistical criteria. Methodological development for practical classes in the discipline "Fundamentals of statistical accounting in ecology" for cadets and students of the direction of training 6.040106 "Ecology, environmental protection and balanced use of nature"]. 10 p. [in Ukrainian]

13. Polotai O.I. (2025) Comparison of operating system features through the prism of cyberattack implementation using the Pearson criterion. In *Svit naukovikh doslidzhen* [World of Scientific Research Mizhnarodna multidistsiplinarna naukova internet-konferentsiya] (pp. 199-202). 26 March, 2025, Ternopil, Ukraine – Opole, Poland [in Ukrainian]

14. Salnikova S. Zastosuvannya kriteriyu Pirsona do viznachennya strukturi testovikh zavdan. [Applying Pearson's criterion to determine the structure of test items] Sotsiologichni studiї - Sociological studies. 78-83. [in Ukrainian]

15. Trofymenko O.G., Dubovoy Y.V. (2018) Regarding the legal potential of the safe functioning of cyberspace. In *Kiberbezpeka v Ukraïni: pravovi ta organizatsiini pitannya* [Cybersecurity in Ukraine: legal and organizational issues: III all-Ukrainian science and practice. conf.] (pp. 5-7). November 30, 2018 Odesa, Ukraine, [in Ukrainian]

Науково-методична стаття.
Надійшла до редакції 30.04.2025.
Прийнято до публікації 04.06.2025.