ВИБІР СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ЦИФРОВІЙ ОСВІТНІЙ ДІЯЛЬНОСТІ

SELECTION OF A SECURITY STRATEGY FOR DIGITAL EDUCATION

Стаття зосереджена на висвітленні питань складності розгортання систем підтримки прийняття рішень в українських закладах вищої освіти для посилення кібербезпеки. Дослідження підкреслює наявність перешкод, що включають в себе проблеми інфраструктурної інтеграції, обмеження ресурсів, бюджетні обмеження. Викладено і надано пояснення емпіричним даним, отриманим в результаті опитувань, проведених серед студентів та викладачів, що виявляють серйозну прогалину в обізнаності про кібербезпеку, а також відсутність ясності щодо протоколів реагування на інциденти. Графічно представлений статистичний аналіз підкреслює кореляції між дефіцитом знань і вразливістю до атак соціальної інженерії. Надано висновок про адаптацію цілісного підходу, який об'єднує технологічні рішення з розширеною освітою користувачів і підготовленістю для розвитку стійкої екосистеми кібербезпеки в українських університетах за обмежених економічних ресурсів.

Ключові слова: *економічні питання, інформаційна безпека, багатокритеріальний аналіз рішень, цифрова освіта, соціальна інженерія, конфіденційність даних, етичні аспекти, поінформованість про безпеку.*

The article focuses on highlighting the complexity of deploying decision support systems in Ukrainian higher education institutions to enhance cybersecurity. The study highlights the presence of significant obstacles to such processes, including infrastructure integration issues, resource constraints, and budget constraints. It also highlights the possibility of using multi-criteria decision analysis, which offers a reliable methodology for finding trade-offs between economic efficiency and security effectiveness, which is crucial in the modern Ukrainian context. The publication expresses the opinion on the possibility of a phased implementation of multi-criteria decision analysis, which includes problem structuring, criteria selection and weighting, alternative evaluation, and final decision-making, specifically adapted to the nuances of the digital education environment. The problem of insufficient funding in higher education institutions is highlighted. The subjectivity and uncertainty in cybersecurity assessments inherent in this area are identified, and the possibility of hybrid methodologies to increase analytical accuracy is also highlighted. Empirical data from surveys conducted among students and faculty are presented and explained, revealing a serious gap in cybersecurity awareness, particularly regarding phishing attacks, as well as a lack of clarity regarding incident response protocols. Graphically presented statistical analysis highlights correlations between knowledge deficits and vulnerability to social engineering attacks. The study clearly highlights the potential of proactive threat detection systems and automated policy adjustments. Ethical implications related to data privacy and algorithm transparency are identified and pointed out. A conclusion is provided on the adaptation of a holistic approach that combines technological solutions with enhanced user education and preparedness for the development of a sustainable cybersecurity ecosystem in Ukrainian universities with limited economic resources.

Key words: *economic issues, information security, multi-criteria decision analysis, digital education, social engineering, data privacy, ethical considerations, security awareness.*

УДК 004.65.056:330.3

DOI: https://doi.org/10.32782/bses.92-5

Синицький Р.К.
аспірант, асистент кафедри
інформаційних систем
в економіці,
Київський національний економічний
університет імені Вадима Гетьмана

Synytskyi Rostyslav
Kyiv National Economic University
named after Vadym Hetman

Постановка проблеми. Однією з основних проблем, пов'язаних із впровадженням системи підтримки прийняття рішень, є складність системи та труднощі інтеграції. Багато навчальних закладів, особливо тих, що мають обмежені ресурси інформаційних технологій, намагаються інтегрувати системи підтримки прийняття рішень з існуючими інфраструктурами кібербезпеки. Технічний досвід, необхідний для налаштування та підтримки систем прийняття рішень, додає ще один рівень складності, ускладнюючи впровадження для установ, які не мають спеціалізованого персоналу. Іншим критичним обмеженням є алгоритмічне зміщення та залежність від даних, де ефективність таких систем залежить від якості та різноманітності вхідних даних. Якщо дані безпеки, які використовуються для навчання моделей штучного інтелекту, є упередженими, застраілими або неповними, система підтримки прийняття рішень може генерувати не правильні оцінки ризиків, які не відображають чітко поточні загрози.

Аналіз останніх досліджень і публікацій. Проблемі дослідження інформаційної безпеки в цифровій освітній діяльності присвячені публікації таких закордонних авторів як D. Magetos, S. Mitropoulos and C. Douligeris [1] та Conteh, Nabie & Schmick, Paul [2]. Проте, маючи майже вичерпний аналіз поданої області дослідження, подібні питання в сучасних реаліях України лишаються відкритими для подальшого дослідження та розвитку.

Постановка завдання. Метою дослідження є аналіз можливості впровадження багатокритеріального аналізу рішень у виборі стратегії інформаційної безпеки та перевірка отриманих результатів на опитуваннях серед сутдентів та викладачів.

Виклад основного матеріалу дослідження. Фінансові наслідки прийняття систем підтримки прийняття рішень становлять доволі серйозну проблему для навчальних закладів, особливо тих, які мають обмежений бюджет. Хоча системи підтримки прийняття рішень пропонує довгострокові переваги з точки зору зменшення ризиків та ефективності роботи, початкові інвестиції в програмне забезпечення, інфраструктуру та навчання можуть бути непомірними. Меншим установам може бути

важко виправдати ці витрати, що призводить до використання традиційних ручних методів оцінки безпеки, які можуть бути не такими ефективними. Крім того, автоматизація прийняття рішень щодо безпеки за допомогою систем підтримки прийняття рішень викликає занепокоєння щодо людського контролю та довіри до автоматизованих рекомендацій. Багато фахівців із кібербезпеки та адміністраторів інформаційних систем можуть не бажати покладатися на керовані алгоритмом рішення щодо безпеки, натомість віддаючи перевагу збереженню людського контролю над критичними процесами безпеки.

Етичні міркування щодо впровадження систем підтримки прийняття рішень також заслуговують на увагу. Збір та аналіз конфіденційних даних користувача викликає занепокоєння щодо конфіденційності, прозорості та підзвітності. Навчальні заклади повинні встановити чітку політику, яка регулює використання даних, гарантуючи, що рішення щодо безпеки, керовані системи підтримки прийняття рішень, не порушують особисті права чи академічну свободу. Крім того, необхідно ретельно контролювати використання автоматизованої оцінки ризиків і прогнозної аналітики в процесі прийняття рішень щодо кібербезпеки, щоб запобігти ненавмисній дискримінації або несправедливому поводженню з користувачами на основі алгоритмічної класифікації. Оскільки системи підтримки прийняття рішень продовжує розвиватися, забезпечення прозорості в процесах прийняття рішень і вирішення потенційних етичних проблем будуть мати вирішальне значення для зміцнення довіри між зацікавленими сторонами.

Значною перевагою багатокритеріального аналізу рішень є його здатність включати як якісні, так і кількісні фактори, що дозволяє університетам оцінювати компроміси між обмеженнями вартості та ефективністю безпеки, що в умовах реалій України з 2019 року є важливим фактором. Додатково, інтеграція даних у режимі реального часу, таких як звіти про інциденти кібербезпеки та записи про фінансові витрати, підвищує надійність моделей багатокритеріального аналізу рішень у адаптації до динамічної і важкопередбачуваної природи загроз цифрової безпеки в Україні. Реалізація багатокритеріального аналізу рішень у виборі стратегії інформаційної безпеки включає кілька ключових етапів: структурування проблеми, вибір критеріїв, призначення ваги, альтернативне оцінювання та остаточне прийняття рішення. Структурування проблеми має вирішальне значення, оскільки воно визначає масштаб і цілі процесу прийняття рішень. У контексті цифрової освіти структурування проблеми обов'язково має враховувати такі фактори, як конфіденційність даних студентів і викладачів, складність інфраструктури інформаційних технологій та вимоги дотримання нормативних вимог.

Вибір критеріїв є кроком, на якому особи, які приймають рішення, визначають ключові атрибути [3], які впливають на ефективність різних стратегій безпеки. Загальні критерії включають фінансові витрати, потенціал зниження ризику, простоту впровадження, вплив на продуктивність системи та масштабованість. Відносна важливість цих критеріїв може змінюватися залежно від інституційних пріоритетів; наприклад, університети з обмеженим бюджетом можуть приділяти більшу вагу економічній ефективності, тоді як науково-дослідні установи, які мають справу з конфіденційними даними, можуть надавати пріоритет зменшенню ризиків.

Тільки після того, як критерії обано та встановлено як необхідні, виконується їх «зважування» для визначення відносної значущості кожного фактора. На цьому кроці можна застосовувати різні методи, такі як попарне порівняння через аналітичний ієрархічний процес або зважування на основі ентропії в інформаційно-теоретичних підходах. «Зважування» або встановлення вагових коефіцієнтів значущості гарантує, що найважливіші критерії мають більший вплив на остаточне рішення не залежно від кількості загально розглянутих критеріїв. Альтернативна фаза оцінки включає оцінку кожної потенційної стратегії безпеки на основі поточно вибарних критеріїв, це можна зробити за допомогою прямих методів підрахунку балів, що є доволі не точною системою оцінки, агрегації думок експертів, що можуть бути упередженими або не мати необхідної кваліфікацій, а також можуть просто помилково надати оцінку через людський фактор, або ж автоматичних механізмів підрахунку балів за допомогою інструментів оцінки ризиків на основі штучного інтелекту, що виключає попередні проблеми.

Ключовим викликом у застосуванні багатокритеріального аналізу рішень до вибору стратегії кібербезпеки є подолання невизначеності та суб'єктивності у прийнятті рішень, та щоб вирішити проблему, були розроблені моделі багатокритеріального аналізу рішень на основі нечіткої логіки [4] для врахування неточних або невизначених вхідних даних. Ці моделі призначають функції приналежності до змінних рішень, що дозволяє більш гнучко відображати фактори ризику безпеки. Наприклад, нечіткий аналітичний ієрархічний процес розширює традиційний шляхом включення лінгвістичних змінних, таких як «високий ризик» або «помірна вартість», які можна кількісно визначити за допомогою нечітких чисел. Більшим удосконаленням традиційних методів багатокритеріального аналізу є інтеграція гібридних моделей, які поєднують кілька методів прийняття рішень для більш надійного аналізу. Наприклад, поєднання аналітичного ієрархічного процесу з аналізом охоплення даних дозволяє університетам свою загальну оцінювати ефективність, порівнюючи результат із найкращими практиками [5]. Подібним

чином гібридні моделі, що включають аналітичний ієрархічний процес і метод порядку переваги за подібністю до ідеального рішення, покращують узгодженість рішень, використовуючи переваги обох методологій мінімізуючі неправильні критерії вибору та покращуючи результат.

У цифровому освітньому середовищі метод порядку переваги за подібністю до ідеального рішення можна застосувати для вирішення різноманітних проблем, пов'язаних із кібербезпекою, включаючи, наприклад, вибір системи виявлення вторгнень, оптимізацію конфігурації брандмауера та оцінку ризиків безпеки в хмарі. Гнучкість багатокритеріального аналізу робить його цінним інструментом для університетів, які прагнуть збалансувати інвестиції в кібербезпеку з операційними обмеженнями. Інтеграція керованих штучним інтелектом систем підтримки прийняття рішень ще більше покращує застосування багатокритеріального аналізу у виборі стратегії кібербезпеки, адже алгоритми машинного навчання можна використовувати для попередньої обробки великих наборів та масивів даних, визначення зв'язків між інцидентами безпеки та впровадженими заходами захисту. Автоматизовані платформи прийняття рішень, які використовують принципи багатокритеріального аналізу, можуть допомогти персоанлу університету, зокрема групам швидкого реагування динамічно коригувати політики безпеки на основі аналізу загроз у реальному часі із швидкою відповіддю від системи підтримки прийняття рішень. Фактично поєднання аналізу рішень, змагального моделювання, оцінки ризиків за допомогою штучного інтелекту та економічної оптимізації забезпечує керований даними, ефективний і економічно ефективний підхід до управління кібербезпекою. Постійна інтеграція штучного інтелекту та розширеної аналітики даних може підвищити точність і адаптивність вибору моделей стратегії безпеки, дозволяючи закладам цифрової освіти залишатися проактивними відносно нових кіберзагроз.

Вибір оптимальної стратегії інформаційної безпеки в цифровій освітній діяльності вимагає великого збору та обробки даних. Від якості, точності та повноти зібраних даних залежить ефективність прийняття рішень. У цьому процесі використовуються три основні джерела інформації: результати тестування на проникнення, опитування, що оцінюють обізнаність студентів і співробітників університету щодо кібербезпеки, і фінансові звіти з детальною інформацією про витрати, пов'язані з безпекою.

Тестування на проникнення є проактивним методом оцінки безпеки, який використовується для оцінки вразливостей цифрових освітніх систем. Університетам варто проводити такі тестування, щоб виявити слабкі місця у своїй інфраструктурі інфомаційних технологій, зокрема вразливості мережі, прогалини в безпеці додатків, неправильні налаштування або нестачу знань у персоналу. Автоматичні інструменти тестування на проникнення, такі як, наприклад Metasploit [6],[7] і Burp Suite [8], мають вбудовані сканери зі структурованими звітами, які класифікують вразливості на основі серйозності, ймовірності використання та потенційного фінансового впливу, що класифікуєтья за шкалою Common Vulnerability Scoring System (рис 1)[9].

Дані, зібрані під час тестування, служать основними вхідними даними для оцінки ризиків безпеки та визначення необхідного рівня інвестицій у захисні заходи.

Звісно існують вдосконалені інструменти тестування на проникнення на основі штучного інтелекту, які можуть ще більше підвищити точність оцінки вразливості шляхом імітації реальних сценаріїв атак, проте вони налаштовані на чисту машинну взаємодію із мережею, виключаючи соціальну інженерію і людський фактор на данному етапі розвитку.

CVSS v4.0 Ratings

Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Рис. 1. Ранжування за Common Vulnerability Scoring System

Джерело: [9]

Такі дані можна згенерувати штучно, на базі статистичних даних, що вже існують у звітах різних компаній зз кібербезпеки, або ж отрмати ще двома різними шляхами, а саме:

- Опитування;
- Тестування на проникненя за лопомогою фішингових-листів.

Було проведено опитування різних респондентів у кількох різних навчальних закладах в місті Києві у період проведення дослідження, адже людський фактор залишається однією з найслабкіших ланок інформаційної безпеки наукових установ і університетів України. Для оцінки рівня обізнаності з питань кібербезпеки серед студентів та співробітників університету було проведено опитування. Проведене опитування допомогло зібрати дані про обізнаність стосовно фішингових атак, звички керування паролями та загальні методи безпеки.

За даними проведеного опитування відомо, що більше 10% опитаних знають або стикались із випадками викрадення саме університетьских

аканутів у викладачів чи викладацького складу освітніх установ, що в результаті могло призвести і доткомпроментації як персональних даних самого викладча, так і до компроментації даних студентів або персоналу через внутрішні системи.

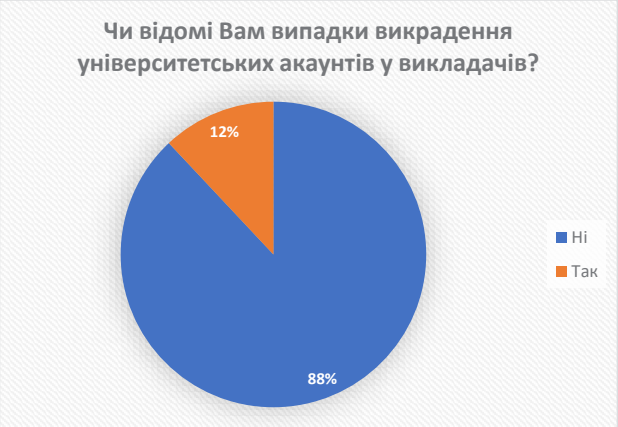

Рис. 2. Статистика опитувань ч.1

Джерело: власне дослідження

Рис. 3. Стастистика опитувань ч. 2

Джерело: власне дослідження

На противагу викладатським зазвичай є менш захищені студенські акаунти, які теж часто стають об'єктом полюваннння або викрадення зловмисників. При тому, що майже той самий відсоток людей не знають, що таке фішинг і як із ним боротись.

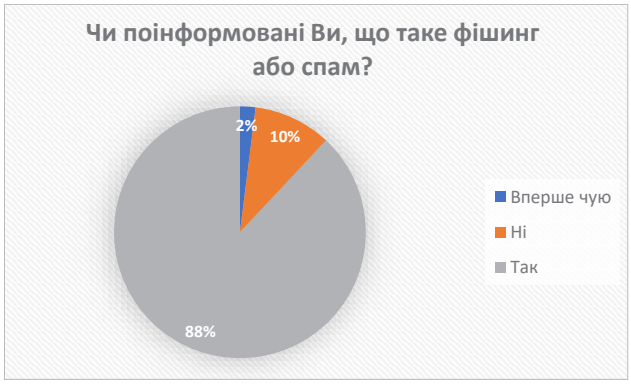

Рис. 4. Стастистика опитувань ч.3

Джерело: власне дослідження

Фактично більше однієї п'ятої респонедентів не знають що робити при викраденні персональних даних, університетських чи персональних акаунтів, що робить кожного п'ятого респондента ідеальною ціллю для атаки.

Рис. 5. Стастистика опитувань ч. 4

Джерело: власне дослідження

Проте, дійсно хорошу інформацію було отриману і питання про команди реагування на інцеденти. Наразі майже 60% респондентів мають до кого звернутись у випадку викрадення даних, втрати університетського акаунту, тощо.

Рис. 6. Стастистика опитувань ч. 5

Джерело: власне дослідження

Якщо подивитись на загальну картину, то матимемо наступну статистику: що 40% респондентів, що поінформоівані про те, що таке фішинг, не мають жодних проблем ні з викраденнями акаунтів, ні з питаннями безпеки (рис. 7).

Статистичний аналіз відповідей на опитування допомагає визначити моделі поведінки, які можуть сприяти ризикам безпеки. Дані, зібрані під час цих опитувань, можна аналізувати для визначення ключових змінних, які впливають на поведінку безпеки. Для виявлення тенденцій і кореляцій зазвичай використовуються такі статистичні методи, як статистичний та регресійний аналіз, а також аналіз головних компонент. Одним із ключових показників, отриманих за результатами

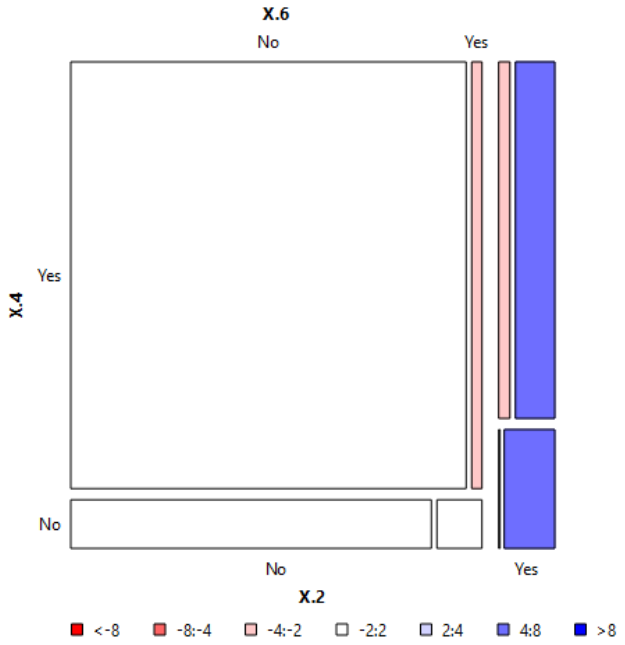

Рис. 7. Стастистика опитувань ч. 6

Джерело: власне дослідження

опитувань щодо обізнаності щодо кібербезпеки, є індекс обізнаності користувачів про аспекти цифрової гігієни та отримання вчасно інформації наприклад, про викрадений акаунт, це довзолило кількісно визначити рівень дотримання найкращих практик безпеки серед різних груп в університеті. Серед іншого, зі статистичного аналізу виявилось, що в той час як студенти напряму зтикались із викраденями персональних або університетських акаунтів, менше полоивни чули про викрадення хоч якихось акаунтів у викладачів, і фактично одиниці дізнавались про втрату акаунту викладачем вчасно, аби не попастись на атаку соціальної інженерії.

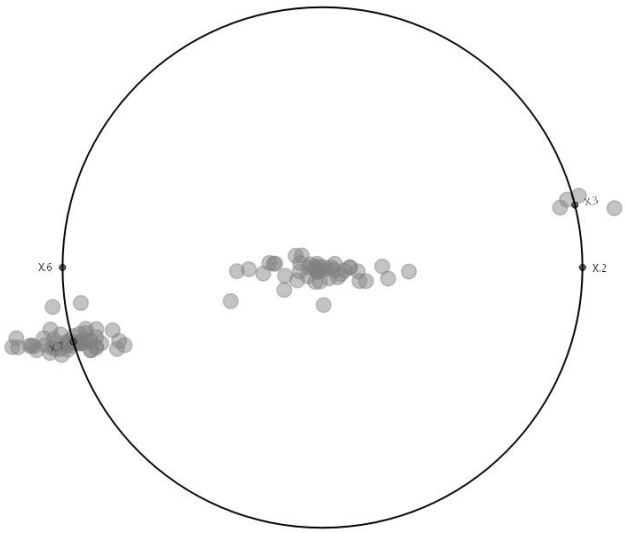

Рис. 8. Стастистика опитувань ч. 7

Джерело: власне дослідження

Збір інформації безпосередньо від студентів і викладачів є доволі важливим аспектом всебічної оцінки безпеки. У дослідженні було використано різні методи для збору даних про поведінку та сприйняття щодо практики кібербезпеки. Основну частину інформації було зібрано за допомогою спостережних досліджень, симуляції фішингових кампаній, обговорень у фокус-групах і механізмів прямого зворотного зв'язку. Імітовані фішингові кампанії надають реальні дані про вразливість студентів і викладачів до атак соціальної інженерії. Такий висновок яскраво продесонстрвано на графіку що створено на основі аналізу головних компонент.

Яскраво видно, що ті, хто знали що таке фішингт і як йому протидіяти не зустрічались у своїй масі з проблемами. Проте, гароню думкою все ж для університетів було б включити інструменти моніторингу на основі штучного інтелекту до системи захисту. Такі інструменти можуть аналізувати частоту надсилання шахрайських електронних листів, визначати, які групи користувачів найбільш уразливі, і рекомендувати стратегії протидії. Зібрані таким чином дані можна включити в навчальні програми з кібербезпеки, щоб підвищити обізнаність і знизити рівень успішності майбутніх атак.

Висновки. Аналіз моделей вибору стратегії безпеки показує, що навчальні заклади використовують різні структури для зниження ризиків, включаючи моделі безпеки на основі оцінки ризиків, моделі, що керуються відповідністю, та адаптивні моделі безпеки. Еволюція цих моделей демонструє зрушення в бік більш динамічних і керованих даними підходів, коли установи використовують аналітику в реальному часі та автоматизацію для підвищення ефективності прийняття рішень щодо безпеки. Традиційні моделі, які ґрунтуються на статичних політиках безпеки, виявилися недостатніми для протидії сучасним кіберзагрозам, які швидко адаптуються та розвиваються. Посилення інтеграції алгоритмів штучного інтелекту і машинного навчання у вибір стратегії безпеки дозволяє установам ефективніше виявляти загрози та реагувати на них. Однак цей перехід створює нові проблеми, зокрема з точки зору конфіденційності даних, етичних міркувань і потенційних упереджень у алгоритмічному прийнятті рішень. На ефективність моделей безпеки додатково впливають інституційна готовність, фінансові обмеження та рівень обізнаності викладачів і студентів щодо кібербезпеки.

Фінансові наслідки прийняття систем підтримки прийняття рішень також становлять проблему для навчальних закладів, особливо тих, які мають обмежений бюджет. Хоча системи підтримки прийняття рішень пропонує довгострокові переваги з точки зору зменшення ризиків та ефективності роботи, початкові інвестиції в програмне забезпечення, інфраструктуру та навчання можуть бути непомірними. Меншим установам може бути важко виправдати

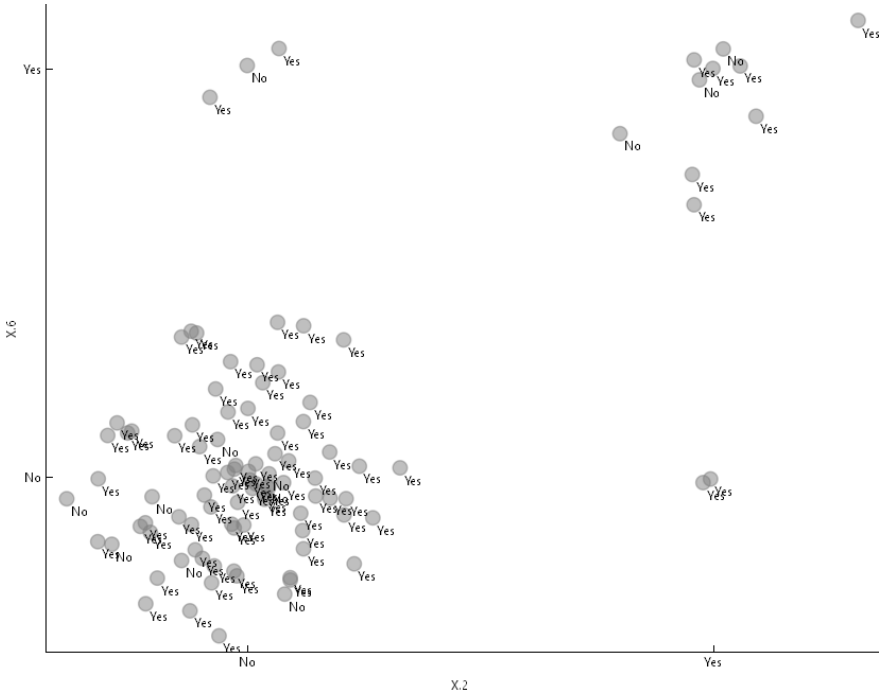

Рис. 9. Стастистика опитувань ч. 8

Джерело: власне дослідження

ці витрати, що призводить до використання традиційних ручних методів оцінки безпеки, які можуть бути не такими ефективними. Крім того, автоматизація прийняття рішень щодо безпеки за допомогою систем підтримки прийняття рішень викликає занепокоєння щодо людського контролю та довіри до автоматизованих рекомендацій. Багато фахівців із кібербезпеки та адміністраторів інформаційних систем можуть не бажати покладатися на керовані алгоритмом рішення щодо безпеки, натомість віддаючи перевагу збереженню людського контролю над критичними процесами безпеки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Magetos D., Mitropoulos S., Douligeris C. Cybersecurity of Distance Education. 2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Athens, Greece. 2024. Pp. 115–120. DOI: https://doi.org/10.1109/SEEDA-CECNSM63478.2024.00029.

2. Conteh N. Y., Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research.* 2016. Vol. 6. P. 31–38. DOI: https://doi.org/10.19101/IJACR.2016.623006.

3. Hussain S.A.I., Mandal U.K., Mondal S P. (2018). Decision Maker Priority Index and Degree of Vagueness Coupled Decision Making Method: A Synergistic Approach. *International Journal of Fuzzy Systems.* 2018. Vol. 20 (5). P. 1551–1566. DOI: https://doi.org/10.1007/s40815-017-0440-9

4. Rane, Nitin & Choudhary, Saurabh. Fuzzy AHP and Fuzzy TOPSIS as an effective and powerful Multi-Criteria Decision-Making (MCDM) method for subjective judgements in selection process. *International Research Journal of 184 Modernization in Engineering Technology and Science.* 2023. Vol. 5. P. 3786–3799. DOI: https://doi.org/10.56726/IRJMETS36629

5. Measuring the Institutional Efficiency Using DEA and AHP the Case of a Mexican University, URL: https://www.elsevier.es/en-revista-journal-applied-research-technology-jart-81-pdf-S1665642314716062 (accessed March 25, 2025).

6. Valea O., Oprisa C. Towards Pentesting Automation Using the Metasploit Framework. 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP). 2020. P. 171–178. DOI: https://doi.org/10.1109/iccp51029.2020.9266234

7. The Metasploit Framework. URL: https://www.metasploit.com/

8. PortSwigger,"BurpSuite".URL:https://portswigger.net/burp

9. NIST, "CVSS: Common Vulnerability Scoring System". URL: https://nvd.nist.gov/vuln-metrics/cvss