International Science Journal of Engineering & Agriculture
2024; 3(4): 93-102
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20240305.09
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Аналіз сучасної наукової думки з дослідження розвитку та протидії кіберзлочинності

Еліна Костянтинівна Доля
студентка, кафедра кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту, Харківський національний університет імені В. Н. Каразіна, Харків, Україна
ORCID 0009-0006-8286-5885

Для цитування цієї статті:
Доля Еліна Костянтинівна. Аналіз сучасної наукової думки з дослідження розвитку та протидії кіберзлочинності. International Science Journal of Engineering & Agriculture. Vol. 3, No.5, 2024, pp. 93-102. doi: 10.46299/j.isjea.20240305.09.
Надійшла до редакції:01 вересня 2024 р.; **Схвалено:** 28 вересня 2024 р.;
Опубліковано: 01 жовтня 2024 р.

Анотація: В роботі проведено аналіз сучасної наукової думки в області кібербезпеки. З'ясовано, що існують різні кіберзлочини й кіберзлочинці часто націлюються на конкретні об'єкти для кібератак з різних причин. Кіберзлочини не обмежені географічними кордонами і можуть відбуватися по всьому світу. Поширеність конкретних видів кіберзлочинності може відрізнятися від країни до країни, залежно від таких факторів, як економічні умови, рівень використання інтернету та загальний розвиток даного явища в регіоні. Фішинг, хакінг, DDoS-атаки, SQL-ін'єкції, експлойти нульового дня, міжсайтові сценарії, атаки на пристрої Інтернету речей (IoT), підробки міжсайтових запитів є поширеними кіберзлочинами у фінансовому секторі в різних країнах із різними методами в розвинених країнах і країнах, що розвиваються. Жертвою кіберзлочинності може стати будь-хто: індивідуальні користувачі Інтернету, підприємства та корпорації, освітні установи, державні установи та інші. Згодом існує багато різних методів навчання кібербезпеці, які застосовуються на практиці. Однак ці зусилля з навчання недостатньо ефективні, і однією з часто згадуваних причин є проблеми з адаптацією користувачів. По суті, користувачі не залучаються до наданого навчання в тій мірі, яка потрібна, щоб отримати від навчання належну користь. У той час як сприйняття та впровадження окремих методів навчання обговорюється в науковій літературі, узгоджені дослідження факторів, які впливають на адаптацію користувачами, є незначними.

Ключові слова: кібербезпека, кіберзлочини, фішинг, DDoS-атаки, інтернет, навчання кібербезпеки.

1. Вступ

Кібербезпека є значним викликом сьогодення, оскільки хакери (кіберзлочинці) завжди намагаються знайти нові методи атаки та використання вразливостей системи [1]. Загрози та ризики для кібербезпеки зросли в останні роки через збільшення кількості підключених пристроїв в мережах. Це призвело до розробки нових шаблонів кібератак, таких як програми-вимагачі, витоки даних і вдосконалені постійні загрози (APT). Отже, для захисту від таких складних атак потрібно враховувати останні системні особливості, щоб створити правильну стратегію захисту кібербезпеки. Центральною темою кібербезпеки є поведінка користувачів, яка, як було показано, є першопричиною або чинником більшості всіх кіберінцидентів, що призводить до потреби надати користувачам можливість прийняти безпечну поведінку.

Дослідники [1] та практики [1,2] сходяться на думці, що вирішальним кроком у наданні користувачам доступу до безпечної поведінки є навчання, саме тому у статті розглядаються сучасні науково-прктичні тенденціїї до питання кібератак, причин їх створення, засоби нанесення збитків від кібератак та шляхи запобігання таким кібератакам.

2. Мета дослідження

Метою дослідження є проведення аналізу сучасної наукової думки в галузі кібербезпеки, визначенні науково обґрунтованих основ напрямків розвитку кіберзагроз й запропоновані сучасниками засоби мінімізації таких кібератак.

3. Методи дослідження

У проведених дослідженнях використовувались методи системного аналізу під час розгляду наукової думки в розглянутих дослідженнях.

Об'єктом дослідження є процес кіберзлочину.

Предметом дослідження є тенденції запобігання кіберзлочинам.

4. Аналіз літератури

У роботі авторів Davidian, M., Kiperberg, M., & Vanetik, N. (2024) [2] та Cen, M., Deng, X., Jiang, F., & Doss, R. (2024) [3] викладено думку про програми-вимагачі, основну сферу їх діяльності та шляхи боротьби з ними. А автори Dennik Baltuttis, & Teubner, T. (2024) [4] виклали дані про здійсненний ними лабораторний експеримент, який мав на меті дослідити стан питання сучасної боротьби з фішингом у бізнес-компаніях. Опублікована Rana Abu Bakar, Lorenzo De Marinis, Cugini, F., & Paolucci, F. (2024) [5] стаття висвітлює DDoS-атак та методи, які були засновані для протидії таним кіберзлочинам. У роботі авторів Lai, T., Farid, F., Bello, A., & Fariza Sabrina (2024) [6] поширено розгляд питання «Інтернет речей» (IoT) та представлено комплексне дослідження використання методів ансамблевого машинного навчання для підвищення кібербезпеки IoT шляхом виявлення аномалій. Автори Arnoldas Budžys, Kurasova, O., & Medvedev, V. (2024) [7] досліджували такі загрози, як витік даних, кібератаки та несанкціонований доступ, загрожують національній безпеці, критичній інфраструктурі та фінансовій стабільності. Розглянуто питання завдання захисту критично важливої інфраструктури від внутрішніх загроз. У роботі авторів Farzana Quayyum, & Letizia Jaccheri (2025) [8] описано «сімейну гру» під назвою «CyberFamily» для сприяння співпраці між батьками та дитиною та підвищення сімейного спілкування з метою підвищення обізнаності дітей віком 9–12 років щодо кібербезпеки. Робота авторів Farzana Quayyum (2024) [9] висвітлює дослідження про стан думки кіберкористувачів дитячого віку до проблем кібербезпеки та ролі батьків у питаннях дотичних із кібербезпекою. Автор Morrow, E. (2024) [10] дослідив методи фішингу, спеціалізовані на закладах вищої освіти. Дослідниками László Bognár, & László Bottyán (2024) [11] викладено дослідження людського чинника й притаманні суспільствам – користквачам кіберпослуг поведінкові фактори, що впливають на практику кібербезпеки студентів, розробляючи надійне, емпірично перевірене опитування. В роботі висвітленої авторами Abdeslam Rehaimi, Yassine Sadqi, Maleh, Y., Gurjot Singh Gaba, & Andrei Gurtov (2024) [12] описано стан хмарних обчислень, які відіграють вирішальну роль у формуванні учнями практичних навичок і розвитку практичного досвіду для захисту від кібератак. А авторів Spatafora, A., Wagemann, M., Sandoval, C., Manfred Leisenberg, & Vaz, C. (2024) [13] привабило глобальне зростання кіберзлочинності підживлюється повсюдною цифровізацією роботи та особистого життя, що посилюється переходом до онлайн-форматів під час пандемії COVID-19. У роботі авторів Cigdem Avci, Bedir Tekinerdogan, & Cagatay Catal (2024) [14] оприлюднено аналіз тактик проектування, які

використовуються для адаптації архітектури Transformer спеціально для проблем кібербезпеки. Робота авторів Wesam Fallatah, Joakim Kävrestad, & Furnell, S. (2024) [15] зосереджена на прийнятті користувачами навчання з кібербезпеки, використовуючи модель прийняття технології як теоретичну основу.

5. Основні сучасні напрями діяльності кіберзлочинності

Приведеним аналізом [1-15] визначено, що сучасна думка кіберзлочинців полягає у декількох основних напрямках їхньої діяльності.

5.1 Програми-вимагачі: що це та який вид їхньої діяльності?

Дослідниками [2-3] зазначено, що програми-вимагачі – це тип зловмисного програмного забезпечення, що набуває все більшої популярності, яке обмежує доступ до системи або даних жертви, доки не буде сплачено викуп.

Традиційні методи виявлення ґрунтуються на аналізі вмісту зловмисного програмного забезпечення, але ці методи неефективні проти невідомого або зловмисного програмного забезпечення «нульового дня». Звичайні засоби захисту від програм-вимагачів часто не можуть виявити атаки програм-вимагачів нульового дня через неможливість заздалегідь отримати підписи програм-вимагачів нульового дня для навчання моделей виявлення. Крім того, атаки програм-вимагачів нульового дня часто використовують складні методи шифрування для атак на нові вразливості, і ці атаки шифрування завдають незворотної шкоди цифровим файлам жертв. Отже, надзвичайно важливо та терміново виявляти атаки невідомих програм-вимагачів на якомога ранішій стадії, в ідеалі до фази шифрування.

5.2 Фішинг: головний глобальний бізнес-ризик

Фішинг - це один з різновидів шахрайства в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів. 96% фішингових атак припадають на електронну пошту. Ще 3% здійснюються через шкідливі сайти і лише 1% — за телефоном.

У роботах [4] автори доводять, що уразливість кібербезпеки належить до головних глобальних бізнес-ризиків. Спроби фішингу, зокрема через електронну пошту, постійно викликають проблеми для організацій, незважаючи на значні інвестиції в IT-безпеку та навчання з підвищення обізнаності. Визнаючи обмеження односторонніх підходів, орієнтованих на технології або людину, це дослідження досліджує, як візуальна індикація ризику може допомогти співробітникам виявити спроби фішингу. Для цього вони провели лабораторний експеримент із відстеженням очей, під час якого учасники оцінювали надійність електронних листів із різними рівнями достовірності. Їх аналіз зосереджується на обробці інформації людиною під час виявлення спроб фішингу, вказуючи на те, що наявність візуального індикатора ризику може суттєво вплинути на поведінку довіри та відповіді, не виводячи з ладу неявні ознаки фішингу (наприклад, явні відправники чи анонімні одержувачі).

Автори дійшли до висновку, що організації повинні належним чином відкалібрувати візуальні індикатори ризику, щоб досягти запланованих керівних ефектів. Однак калібрування залишається компромісом і залежить від середовища організації.

5.3 Атаки відмови в обслуговуванні (DoS) та розподілені атаки відмови в обслуговуванні (DDoS)

У роботі [5] зазначено, що розподілені атаки типу «відмова в обслуговуванні» (DDoS) є основною загрозою для комп’ютерних мереж . Ці атаки можуть бути здійснені шляхом заповнення мережі зловмисним трафіком, перевантаження її ресурсів та/або роблячи її

недоступною для законних користувачів. Існуючі методи машинного навчання для виявлення атак DDoS зазвичай використовують статистичні характеристики мережевого трафіку, наприклад розміри пакетів і час між надходженнями. Однак ці методи часто не в змозі вловити складні відносини між різними потоками трафіку. У цьому рукописі пропонується новий підхід до виявлення атак DDoS, який використовує ансамблеве навчання графових нейронних мереж (GNN). Ансамблеве навчання GNN – це тип машинного навчання, який поєднує кілька моделей GNN для підвищення точності виявлення. Вони оцінили підхід на наборі даних Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset (CICIDS2018) і (CICIDS2017), який є еталонним набором даних для виявлення атак DDoS. Їх робота дає два основні внески. По-перше, вони розширюють підхід до виявлення атак DDoS за допомогою навчання ансамблю GNN. По-друге, вони досліджують оцінку та точне налаштування показників гіперпараметрів за допомогою ансамблевого навчання, значно підвищуючи точність порівняно з окремою моделлю GNN і досягаючи в середньому на 3,2% вищого результату F1. Крім того, їх підхід ефективно зменшує переобладнання завдяки використанню методів регулярізації, таких як відмова та рання зупинка. Зокрема, вони використовують ієрархічний ансамбль GNN, де кожен GNN вивчає зв'язки між потоками трафіку на різному рівні деталізації. Потім вони використовують пакетування та посилення, щоб поєднати передбачення окремих GNN, ще більше покращуючи точність виявлення. Результати показують, що їх система може досягти 99,67% точності з показником F1 99,29%, що краще, ніж найсучасніші методи, навіть якщо використовувати єдину архітектуру трафіку.

5.4 Атаки на пристрої Інтернету речей (IoT)

У роботі [6] зазначено, що Інтернет речей (IoT) об'єднує понад мільярди інтелектуальних пристроїв по всьому світу з можливістю обміну даними з іншими підключеними пристроями практично без втручання людини. IoT дозволяє агрегувати та аналізувати дані у великому масштабі, щоб покращити якість життя в багатьох сферах. Зокрема, дані, зібрані IoT, містять величезну кількість інформації для виявлення аномалій. Гетерогенна природа IoT є одночасно викликом і можливістю для кібербезпеки. Традиційні підходи до моніторингу кібербезпеки часто вимагають різних типів попередньої обробки та обробки даних для різних типів даних, що може бути проблематичним для наборів даних, які містять різнорідні характеристики. Однак різнорідні типи мережевих пристроїв часто можуть фіксувати більш різноманітний набір сигналів, ніж зчитування одного типу пристрою, що особливо корисно для виявлення аномалій. У статті [6] представлено комплексне дослідження використання методів ансамблевого машинного навчання для підвищення кібербезпеки IoT шляхом виявлення аномалій. Замість того, щоб використовувати одну модель машинного навчання, ансамблеве навчання поєднує в собі передбачувану силу кількох моделей, підвищуючи їх точність прогнозування в різнорідних наборах даних замість використання однієї моделі машинного навчання. Вони пропонують уніфіковану структуру з ансамблевим навчанням, яка використовує байєсівську оптимізацію гіперпараметрів для адаптації до мережевого середовища, яке містить численні показання датчиків IoT. Експериментально вони продемонстрували їх високу прогностичну силу порівняно з традиційними методами.

5.5 Інсайдерські атаки – авторизований доступ до системи

Роботи [6-7] автори стверджують, що у сучасному кіберсередовищі такі загрози, як витік даних, кібератаки та несанкціонований доступ, загрожують національній безпеці, критичній інфраструктурі та фінансовій стабільності. Це дослідження стосується складного завдання захисту критично важливої інфраструктури від внутрішніх загроз через високий рівень довіри та доступу, який зазвичай отримують ці люди. Інсайдери можуть отримати пароль системного адміністратора шляхом ретельного спостереження або шляхом розгортання програмного

забезпечення для збору інформації. Щоб вирішити цю проблему, пропонується інноваційна методологія на основі штучного інтелекту для ідентифікації користувача за динамікою натискання пароля. У рукописі [7] представлено новий метод перетворення матриці фільтра Габора для перетворення числових значень у зображення шляхом виявлення поведінкової моделі введення пароля. Сіамська нейронна мережа (SNN) із розгалуженнями згорткових нейронних мереж використовується для порівняння зображень з метою виявлення несанкціонованих спроб доступу до систем критичної інфраструктури. Мережа аналізує унікальні особливості часових позначок пароля користувача, трансформованих у зображення, і порівнює їх із раніше надісланими паролями користувачів. Отримані результати вказують на те, що перетворення числових значень динаміки натискання клавіш у зображення та навчання SNN призводить до нижчого рівня рівних помилок (EER) і вищої точності автентифікації користувача, ніж раніше повідомлялося в інших дослідженнях. Методологію перевірено на загальнодоступних колекціях динаміки натискань клавіш, наборах даних CMU та GREYC-NISLAB, які разом містять понад 30 000 зразків паролів. Він досягає найнижчого значення EER 0,04545 порівняно з найсучаснішими методами перетворення неграфічних даних у зображення.

6. Результати дослідження

6.1 Навчання дітей та батьків у сфері кібербезпеки

Автори статей [8-9] стверджують, що участь батьків є суттєвим фактором, який впливає на навчання, поведінку та будь-які інші аспекти життя дитини, включаючи спілкування в Інтернеті. Вважаючи батьків відповідальними за наслідки дій дітей в Інтернеті та загальне благополуччя, вони часто ігнорують важливість і потребу в засобах, які можуть ефективно підтримувати батьків у взаємодії та участі в діяльності зі своїми дітьми. У цьому дослідженні вони описують та оцінюють спільну сімейну гру під назвою «CyberFamily» для сприяння співпраці між батьками та дитиною та підвищення сімейного спілкування з метою підвищення обізнаності дітей віком 9–12 років щодо кібербезпеки. Вони також представили результати двох досліджень користувачів: одне, проведене з чотирма діадами «батько-діти», щоб перевірити доцільність гри, і друге дослідження, проведене за участю 11 діад «батьки-діти», зосереджене на оцінці зручності використання CyberFamily. Їх висновки дали позитивний відгук і показали, що спільна сімейна гра, така як CyberFamily, може допомогти батькам залучити дітей до діяльності в Інтернеті, що призведе до обговорень і потенціалу для спільного навчання для обох груп. Вони пропонують, щоб майбутні дослідники та дизайнери розглянули та забезпечили активну, залучену роль батьків при розробці рішень для підвищення обізнаності дітей про кібербезпеку, а не просто змушували батьків доступ дітей до Інтернету.

Технології спільного проектування та спільного створення нещодавно привернули велику увагу в спільноті взаємодії дітей з комп’ютером (CCI). Однак автори статті [9] стверджують, що ще потрібно багато працювати над вивченням аспекту спільного проектування у сфері обізнаності дітей про кібербезпеку та залучення батьків. У цьому дослідженні вони представили результати спільного проектування за участю десяти дітей віком від 9 до 12 років, щоб дослідити, як діти думають про різні проблеми кібербезпеки та ролі батьків у цих ситуаціях, пов’язаних з кібербезпекою. Їх висновки показують, що діти очікують, що різні ролі дорослих нададуть підтримку для забезпечення їхньої безпеки в Інтернеті, і особливо очікують, що їхні батьки виконають роль підтримки в умовах кібербезпеки, інформуючи їх про ризики, пропонуючи пропозиції щодо пом’якшення чи захисних заходів і допомагаючи їм вжити заходів захисту заходи або дії проти будь-якої особи, що становить ризик. Їх дослідження сприяє розумінню сприйняття дітьми кібербезпеки та участі батьків через розповідь історій.

6.2 Навчання студентів вищих навчальних закладів у сфері кібербезпеки

Університети часто стають об'єктами кібератак. Дослідження авторів [10] ставить метою своєї роботи вивчити поширені методи фішингу, націлені на заклади вищої освіти. Це дослідження аналізує вміст і особливості повідомлень вибірки з 2300 електронних листів з 2010 по 2023 рік, зібраних із Cornell Phish Bowl, включаючи теми, переконливі заклики, емоційні заклики та орфографічні помилки. Використовуючи аналіз зв'язків і видобуток тексту, робота визначає зміни тенденцій фішингу з часом. Одним з головних висновків є те, що фішинг, зосереджений на безпеці, замінений тим, хто намагається відобразити повсякденне університетське життя, наприклад шахрайство з пропозиціями роботи. Крім того, це дослідження визначає авторитетність і дефіцит як звичайні переконливі заклики під час спроб фішингу та демонструє зменшення кількості орфографічних помилок з часом. Ці висновки мають практичне значення для навчання та підвищення обізнаності з кібербезпеки. Вони також можуть керувати майбутньою роботою з визначення вразливості користувачів до фішингу, надаючи інформацію про часті атаки.

Оскільки цифрова епоха проникає у вищу освіту, обізнаність студентів університетів щодо кібербезпеки стала актуальною проблемою. Це дослідження [11] вивчає поведінкові фактори, що впливають на практику кібербезпеки студентів, розробляючи надійне, емпірично перевірене опитування. У їх дослідженні застосовано комплексну структуру, яка використовує дослідницький і підтверджуючий факторний аналіз (EFA; CFA), щоб підтвердити здатність опитування охопити складні аспекти обізнаності студентів щодо кібербезпеки. Модель структурного рівняння (SEM) була розроблена для окреслення та ретельного вивчення п'яти ключових аспектів поведінки студентів у сфері кібербезпеки. Після перевірки вони використали цю модель для проведення ретельного порівняльного аналізу поведінки щодо кібербезпеки серед представників різноманітної демографічної групи студентів, які брали участь в опитуванні. Розслідування включало вивчення поведінки за статтю, віковими групами, академічними дисциплінами та культурним походженням, проливаючи світло на різноманітну поведінку щодо кібербезпеки, яка визначає досвід сучасних студентів. Їх дослідження, зрештою, прагне зробити внесок у підвищення цифрової безпеки в освітньому середовищі, узгоджуючи онлайн-практику студентів із надійними заходами безпеки та виховуючи культуру кібербезпеки в академічних колах.

Автори статті [12] стверджують, концепції хмарних обчислень (CC) і віртуалізації — це дві передові технології, запроваджені для розширення можливостей дистанційного та змішаного навчання. Крім того, вони відіграють вирішальну роль у формуванні учнями практичних навичок і розвитку практичного досвіду для захисту від кібератак. Багато вищих навчальних закладів (ВНЗ) у розвинених країнах уже прийняли обіцянку CC підвищити освітні стандарти. Однак темпи його впровадження в країнах, що розвиваються, стагнують. Крім того, існуючі рішення в літературі не є стійкими. Вони або покладаються на локальну інфраструктуру, або пов'язані з одним постачальником хмарних послуг. Отже, вони, ймовірно, схильні до збоїв і раптового відключення. Щоб заповнити цю прогалину, ця стаття є першою, яка комплексно розглядає вищезазначені проблеми та представляє об'єднану гібридну систему CC на основі розширення Apache Virtual Computing Lab (VCL). Запропонована система забезпечує незалежну реалізацію з відкритим кодом, більшу гнучкість конфігурації та методологічні вдосконалення порівняно з існуючими дослідженнями в літературі. Крім того, це сприяє стабільності служб CC, розширюваної хмарної архітектури та відмовостійкості. VCL в основному зосереджена на створенні віртуальних лабораторій (VL) для дистанційної освіти з кібербезпеки та комп'ютерних мереж, з потенційним розширенням на інші сфери інженерної освіти. Крім того, у цьому документі представлено GPT-TerminalPro, інструмент на базі терміналу, керований Generative Pretrained Transformer (GPT-3.5) OpenAI, який надає інтелектуальну допомогу користувачам під час виконання лабораторних завдань. Щоб експериментально оцінити продуктивність VCL, використовуються стандартні інструменти

Linux, а також тест Apache і HTTP-генератори навантаження httperf. VCL було протестовано з 30 користувачами та 61 віртуальним обчислювальним середовищем користувача, щоб підтвердити загальну продуктивність. Результати вражають: час ініціалізації, включаючи всі фонові завдання VCL, завжди становить менше хвилини та використовує менше обчислювальних ресурсів, забезпечуючи кращу взаємодію з користувачем. Цей документ сприятиме прийняттю CC у країнах з низьким рівнем доходу.

6.3 Обізнаність у сфері кібербезпеки, огляд на рівні малого та середнього бізнесу

Глобальне зростання кіберзлочинності підживлюється повсюдною цифровізацією роботи та особистого життя, що посилюється переходом до онлайн-форматів під час пандемії COVID-19. Із розвитком цифрових каналів зростають і можливості для кібератак, особливо тих, які наражають малі та середні підприємства (МСП) на потенційну економічну руйнацію. Ці підприємства часто не мають комплексних оборонних стратегій та/або необхідних ресурсів для впровадження ефективних заходів кібербезпеки. Автори [13] вирішили цю проблему, розробивши освітню кімнату квесту (EER), яка підтримує навчання на основі сценаріїв для підвищення обізнаності про кібербезпеку серед працівників малого та середнього бізнесу, дозволяючи їм ефективніше справлятися з кіберзагрозами. Інтегруючи практичні сценарії, засновані на прикладах із реального життя, автори прагнули покращити збереження знань і операційну продуктивність персоналу малого та середнього бізнесу з точки зору кібербезпечних практик. Результати, отримані під час пілотного тестування з понад 200 учасниками, свідчать про те, що підхід EER залучив слухачів і підвищив їхню обізнаність щодо кібербезпеки, що стало кроком вперед у навчанні з кібербезпеки.

У середовищі кіберзагроз, що швидко розвивається, ефективні стратегії захисту є вирішальними для захисту конфіденційної інформації та критично важливих систем. Методи глибокого навчання, зокрема архітектура Transformer, показали величезний потенціал у вирішенні проблем кібербезпеки. Однак налаштування та адаптація архітектури Transformer для додатків кібербезпеки є проблемою, яка вимагає використання ефективних стратегій для досягнення оптимальної продуктивності. У дослідженні [14] представлено комплексний аналіз тактик проектування, які використовуються для адаптації архітектури Transformer спеціально для проблем кібербезпеки. Тактика проектування, яка визначається як стратегічні рішення архітектурних проблем на основі добре обґрунтованих проектних рішень, детально досліджується в контексті кібербезпеки. Вивчаючи модифікації та адаптації, внесені до оригінальної архітектури Transformer, це дослідження розкриває дизайнерські рішення та стратегії, важливі для успішного впровадження в різноманітних сферах кібербезпеки. Результати підкреслюють важливість узгодження тактики проектування з унікальними бізнес-вимогами та факторами якості кожної конкретної області застосування. Це дослідження містить цінну інформацію про використання тактики проектування для налаштування архітектури Transformer у сфері кібербезпеки, прокладаючи шлях для розширених стратегій захисту від динамічної та постійної природи кіберзагроз.

7. Результати досліджень

Кібербезпека вважається основоположною для організацій і окремих осіб, які працюють з цифровими технологіями. Центральною темою кібербезпеки є поведінка користувачів, яка, як було показано, є першопричиною або чинником більшості всіх кіберінцидентів, що призводить до потреби надати користувачам можливість прийняти безпечну поведінку. Дослідники та практики сходяться на думці, що вирішальним кроком у наданні користувачам доступу до безпечної поведінки є навчання. Згодом існує багато різних методів навчання кібербезпеці, які обговорюються в науковій літературі та застосовуються на практиці. Однак дослідження свідчать про те, що ці зусилля з навчання недостатньо ефективні, і однією з часто згадуваних

причин є проблеми з адаптацією користувачів. По суті, користувачі не залучаються до наданого навчання в тій мірі, яка потрібна, щоб отримати від навчання належну користь. У той час як сприйняття та впровадження окремих методів навчання обговорюється в науковій літературі, узгоджені дослідження факторів, які впливають на адаптацію користувачами, є незначними. З цією метою стаття [15] зосереджена на прийнятті користувачами навчання з кібербезпеки, використовуючи модель прийняття технології як теоретичну основу. На основі 22 включених публікацій дослідження містить огляд факторів прийнятності для навчання з кібербезпеки, які обговорювалися в існуючій науковій літературі. Основний внесок — це цілісна компіляція наявних знань про фактори, які впливають на сприйняття користувачами навчання з кібербезпеки, і впровадження CTAM, моделі прийняття навчання з кібербезпеки, яка визначає чотири фактори — регулятивний контроль, занепокоєння, апатія та довіра — які впливають на користувачів ' намір прийняти навчання з кібербезпеки. Результати можуть бути використані для спрямування майбутніх досліджень, а також для практиків, які впроваджують навчання з кібербезпеки.

8. Перспективи подальшого розвитку досліджень

Організації, які впроваджують обізнаність про кібербезпеку, повинні прагнути позитивно змінити ставлення та поведінку працівників. Однак на практиці більшість таких ініціатив лише підвищують знання працівників. У сфері кібербезпеки знання самі по собі не матимуть суттєвої цінності, якщо вони не будуть використовуватися для прийняття рішень і спонукання до дій. Таким чином, це дослідження вивчало атрибути, які можуть впливати на позитивні зміни в поведінці співробітників щодо кібербезпеки та сприяти цим. Ці атрибути є такими:

- отримати підтримку керівництва та участь у діяльності CSA;
- розглядати CSA як безперервний процес, який потребує регулярного оновлення та вдосконалення;
- культивувати та поширювати «кібербезпеку» як норму в організації;
- заохочувати дії та поведінку з кібербезпеки за допомогою стимулів;
- створювати та використовувати переконливі повідомлення CSA;
- використовувати інноваційні та ефективні підходи до поширення повідомлень CSA;
- рекомендувати заходи безпеки, які є досяжними та актуальними для аудиторії.

9. Висновки

Аналіз сучасної наукової думки до питання довів актуальність теми кіберзлочинності й її дослідження. Визначено, що кібербезпека є актуальним питанням різних галузей діяльності людства. Доведено проведеним аналізом й приналежність до учасників убезпечення даних від злочинців користувачів кіберпростору від дев’яти років.

До основних напрямів кіберзлочинної діяльності можна віднести: Фішинг, хакінг, DDoS-атаки, SQL-ін’єкції, експлойти нульового дня, міжсайтові сценарії, атаки на пристрої інтернету речей (IoT), підробки міжсайтових запитів (CSRF).

Сучасними дослідженнями виявлено наступний напрям протидії кіберзлочинності: потрібно багато працювати над вивченням аспекту спільного проектування у сфері обізнаності дітей, батьків та працівників бізнесу про кібербезпеку та протидії кіберзлочинності; рекомендувати заходи безпеки, які є досяжними та актуальними для аудиторії;

Список літератури:

1) Grace Odette Boussi, Gupta, H., & Syed Akhter Hossain. (2024). A machine learning model for predicting phishing websites. International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, 14(4), 4228–4228. https://doi.org/10.11591/ijece.v14i4.pp4228-4238

2) Davidian, M., Kiperberg, M., & Vanetik, N. (2024). Early Ransomware Detection with Deep Learning Models. Future Internet, 16(8), 291–291. https://doi.org/10.3390/fi16080291

3) Cen, M., Deng, X., Jiang, F., & Doss, R. (2024). Zero-Ran sniff: A zero-day ransomware early detection method based on zero-shot learning. Computers & Security, 142, 103849–103849. https://doi.org/10.1016/j.cose.2024.103849

4) Dennik Baltuttis, & Teubner, T. (2024). Effects of Visual Risk Indicators on Phishing Detection Behavior: An Eye-Tracking Experiment. Computers & Security, 103940–103940. https://doi.org/10.1016/j.cose.2024.103940

5) Rana Abu Bakar, Lorenzo De Marinis, Cugini, F., & Paolucci, F. (2024). FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection. Computer Networks, 250, 110508–110508. https://doi.org/10.1016/j.comnet.2024.110508

6) Lai, T., Farid, F., Bello, A., & Fariza Sabrina. (2024). Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis. Cybersecurity, 7(1). https://doi.org/10.1186/s42400-024-00238-4

7) Arnoldas Budžys, Kurasova, O., & Medvedev, V. (2024). Deep learning-based authentication for insider threat detection in critical infrastructure. Artificial Intelligence Review, 57(10). https://doi.org/10.1007/s10462-024-10893-1

8) Farzana Quayyum, & Letizia Jaccheri. (2025). CyberFamily: A collaborative family game to increase children's cybersecurity awareness. Entertainment Computing, 52, 100826–100826. https://doi.org/10.1016/j.entcom.2024.100826

9) Farzana Quayyum. (2024). Co-designing cybersecurity-related stories with children: Perceptions on cybersecurity risks and parental involvement. Entertainment Computing, 100753–100753. https://doi.org/10.1016/j.entcom.2024.100753

10) Morrow, E. (2024). Scamming Higher Ed: An Analysis of Phishing Content and Trends. Computers in Human Behavior, 108274–108274. https://doi.org/10.1016/j.chb.2024.108274

11) László Bognár, & László Bottyán. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. Education Sciences, 14(6), 588–588. https://doi.org/10.3390/educsci14060588

12) Abdeslam Rehaimi, Yassine Sadqi, Maleh, Y., Gurjot Singh Gaba, & Andrei Gurtov. (2024). Towards a federated and hybrid cloud computing environment for sustainable and effective provisioning of cyber security virtual laboratories. Expert Systems with Applications, 124267–124267. https://doi.org/10.1016/j.eswa.2024.124267

13) Spatafora, A., Wagemann, M., Sandoval, C., Manfred Leisenberg, & Vaz, C. (2024). An Educational Escape Room Game to Develop Cybersecurity Skills. Computers, 13(8), 205–205. https://doi.org/10.3390/computers13080205

14) Cigdem Avci, Bedir Tekinerdogan, & Cagatay Catal. (2024). Design tactics for tailoring transformer architectures to cybersecurity challenges. Cluster Computing. https://doi.org/10.1007/s10586-024-04355-0

15) Wesam Fallatah, Joakim Kävrestad, & Furnell, S. (2024). Establishing a Model for the User Acceptance of Cybersecurity Training. Future Internet, 16(8), 294–294. https://doi.org/10.3390/fi16080294

Analysis of modern scientific opinion on the study of the development and counteraction of cybercrime

Elina Dolia
Education and Research Institute of Computer Sciences and Artificial Intelligence, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID 0009-0006-8286-5885

Abstract: The work provides an analysis of modern scientific thought in the field of cyber security. It has been found that there are different cybercrimes and cybercriminals often target specific targets for cyberattacks for different reasons. Cybercrimes are not limited by geographical boundaries and can occur all over the world. The prevalence of specific types of cybercrime can vary from country to country, depending on factors such as economic conditions, the level of Internet use and the general development of the phenomenon in the region. Phishing, hacking, DDoS attacks, SQL injections, zero-day exploits, cross-site scripting, attacks on Internet of Things (IoT) devices, cross-site request forgery (CSRF) are common cybercrimes in the financial sector in different countries with different methods in developed countries and developing countries. Anyone can become a victim of cybercrime: individual Internet users, businesses and corporations, educational institutions, government agencies, and others. Subsequently, there are many different methods of cyber security training that are put into practice. However, these training efforts are not effective enough, and one of the often cited reasons is user onboarding issues. Essentially, users are not engaging with the training provided to the extent necessary to get the proper benefit from the training. While the acceptance and implementation of particular training methods is discussed in the scientific literature, there is little coherent research on the factors that influence user adaptation.

Keywords: cyber security, cyber crimes, phishing, DDoS attacks, Internet, cyber security training.