ВИДИ КІБЕРЗАГРОЗ ТА ВАЖЛИВІСТЬ ВИВЧЕННЯ ОСНОВ КІБЕРБЕЗПЕКИ

Суков Михайло Валерійович
здобувач вищої освіти бакалаврського рівня
sukov5363@gmail.com
Кручинська Дар'я Романівна
асистент
Кафедра комп'ютерних наук та інформаційних технологій
dashaqwerty1@gmail.com
Житомирський державний університет імені Івана Франка, Україна

Кібербезпека набуває все більшої актуальності в сучасному світі. З розвитком цифрових технологій зростає і потенційна загроза кібератак. Саме тому важливо підкреслити необхідність вивчення кібербезпеки та заходів, які можуть застосовувати окремі особи та організації для захисту від кіберзагроз.

Перш за все, слід розуміти важливість кібербезпеки. Кібератаки можуть призводити до викрадення особистої та конфіденційної інформації, фінансових втрат і навіть пошкодження критично важливої інфраструктури. Оскільки наша залежність від цифрових технологій зростає, потенційний вплив кібератак стає все серйознішим. Тому дуже важливо, щоб окремі особи та організації вживали заходів для свого захисту.

Мета статті - розглянути основні види кіберзагроз та підкреслити важливість вивчення основ кібербезпеки.

Дослідження вчених і практиків підтверджують, що професійна підготовка фахівців у сфері кібербезпеки є ключовим напрямом державної політики у сфері національної безпеки і оборони. Без цього неможливо забезпечити захищене передавання інформації, а отже, і науково-технічний та соціально-економічний розвиток країни. Аналіз академічних праць показує, що в умовах інформаційних воєн та загроз цілісності й суверенітету України питання підготовки фахівців із кібербезпеки охоплюють педагогічні, системні та міждисциплінарні аспекти. Останні дослідження та публікації свідчать, що проблеми професійного розвитку фахівців з кібербезпеки залишаються недостатньо дослідженими.

За даними сайту slovoidilo.ua, минулого року на українські новинні портали було здійснено 2543 кібератаки. За даними урядової групи реагування на комп'ютерні надзвичайні ситуації CERT-UA, зафіксовано 347 кібератак проти уряду та державних організацій, 276 – проти органів місцевого самоврядування, 175 – проти організацій у сфері безпеки та оборони та 127 випадків проти комерційних організацій. Ще 92 атаки було здійснено на енергетичну галузь, 81 атаку на телекомунікації, 38 атак на навчальні заклади, 32 атаки на транспортну галузь, 30 атак на фінансову галузь, 25 атак на ІТ-галузь, 15 випадків у ЗМІ та 12 справ у медичних закладах. Лише за другу половину 2023 року було зафіксовано та розслідувано 1500 кіберінцидентів.[1]

Кіберпростір залишається місцем постійних викликів і можливостей. У результаті кібератаки, вимагання та витік даних набирають обертів, стаючи проблемою як для окремих осіб, так і для великих організацій. Захист даних і безпека системи повинні бути головним пріоритетом для кожного з нас. Згідно з припущеннями h-x.technology, до 2024 року ми і світ прогнозуємо, що кількість кібератак зросте на 15%, атак, спрямованих на отримання конфіденційних даних, зросте мінімум на 18%, до 2000 атак. Середня вартість витоку даних становитиме щонайменше 4,5 мільйона доларів. Кількість атак програм-вимагачів зросте через появу нових вразливостей і, отже, нових можливостей. Також будуть організовані нові великі групи розробників програм-вимагачів. З урахуванням тенденцій останніх років їх очікувана кількість зростає до 70-75. Фішингові атаки спрямовані на шпигунство та доступ до системи. Дані атаки збільшаться через використання вкрадених облікових даних, а штучний інтелект вдосконалить і персоналізує такі атаки. Ці два фактори зроблять фішингові атаки ефективнішими, менш помітними та, перш за все, більш частими. Основною метою фішингових атак наступного року стануть фінансові установи, а каналами – електронна пошта, соціальні мережі та SaaS (програмне забезпечення як послуга). DDoS-атаки та фішингові атаки зростатимуть на тлі нестабільної світової геополітичної ситуації. DDoS-атаки (розподілена атака на відмову в обслуговуванні) призведуть до припинення медіа, громадських служб, транспорту, фінансових та інших державних установ. Очікувана кількість масштабних DDoS-атак у 2024 році становитиме близько 2 мільйонів. Кіберзлочинність також зросте через заплановані вибори в США, Великобританії та Індії. Ця ситуація стане

можливістю для багатьох типів кіберзлочинців створити нестабільне середовище та порушити демократичний процес. Кіберзлочинці зосередяться на нових цілях: хмарних ресурсах, штучному інтелекті та криптовалютах. GPU Farming стане популярною мішенню у сфері хмарних кібератак. Пріоритетом буде використання штучного інтелекту як кіберзлочинцями для розробки нових атак, так і організаціями кіберзахисту. Щоб отримати доступ до великих цільових організацій, кіберзлочинці продовжуватимуть використовувати вразливості не лише в системах безпеки цих організацій, але й у системах безпеки великих постачальників і хмарних постачальників. Критичною потребою організацій є вдосконалення інструментів безпеки, процесів і протоколів, особливо в області захисту ланцюга передавання даних. Організації зосередяться на розвитку кіберстійкості для швидкого відновлення та мінімізації втрати даних, оскільки неможливо захистити на 100% від кібератак. Ринок кіберстрахування зростатиме.[2]

Як зазначають у SecurityWeek, через збільшення кіберзагроз організаціям потрібні більш кваліфіковані спеціалісти з кібербезпеки. Цей попит створює сприятливі умови для тих, хто хоче розвиватися в цій галузі. Згідно з дослідженнями, ринок праці в сфері кібербезпеки швидко зростає, пропонуючи високі зарплати та багато можливостей для професійного зростання. Фахівці з кібербезпеки можуть працювати в різних секторах економіки, включаючи фінансові установи, медичні організації, державні структури та багато інших. Кожен з цих секторів має свої специфічні вимоги до безпеки даних, що відкриває широкий спектр кар'єрних можливостей. Більше того, багато організацій готові інвестувати у підвищення кваліфікації своїх співробітників, що робить навчання кібербезпеці ще більш привабливим.[3]

В таких реаліях організації змушені запроваджувати нові підходи до кібербезпеки, щоб ефективно захистити свої дані. Одним із таких підходів є «архітектура нульової довіри», яка вимагає ретельної перевірки кожного користувача та пристрою, які намагаються отримати доступ до ресурсів організації. Для кращого розуміння, потрібно розібратись, що таке «архітектура нульової довіри». Як пишуть на wikipedia.org: ”Модель з нульовою довірою (англ. zero trust model) — модель побудови інформаційних систем, що виходить з того, що систему вже зламано, і тому довіряти не можна нікому, навіть легітимним користувачам усередині периметра. А отже, кожен доступ до даних і програм потребує підтвердження. Окрім того, модель передбачає видачу користувачам лише мінімально необхідних привілеїв, а також профілювання їх поведінки для подальшого виявлення аномалій та загроз.”. Тому впровадження такої архітектури вимагає глибоких знань і навичок у сфері кібербезпеки, що підкреслює важливість відповідного навчання. Професіонали з цими знаннями стали незамінними для організацій, які прагнуть захистити свої дані від сучасних загроз.[4]

Сучасні технології, такі як штучний інтелект, блокчейн і квантові обчислення, також впливають на кібербезпеку, адже його можуть використовувати не тільки для вчинення злочинів, а й для захисту даних.

Навчання в цій галузі включає вивчення новітніх технологій та їх впливу на безпеку даних. Це дозволяє експертам бути на крок попереду кіберзлочинців і ефективно захищати організації від нових загроз. Блокчейн забезпечує високий рівень безпеки завдяки своїй децентралізованій природі, що робить його привабливим для багатьох галузей. Однак він не є повністю безпечним, тому експерти з кібербезпеки повинні розуміти його вразливості та способи їх усунення. З іншого боку, квантові обчислення можуть як підвищити безпеку за допомогою складних алгоритмів шифрування, так і створити нові загрози, які слід враховувати в майбутньому.

Освіта в сфері кібербезпеки сприяє формуванню обізнаності про безпечну поведінку в Інтернеті. Учні та студенти навчаються використовувати складні паролі, методи двофакторної аутентифікації та інші засоби захисту, що допомагають запобігти несанкціонованому доступу до їхніх акаунтів і особистої інформації. Ці навички стають фундаментальними для безпечного користування цифровими технологіями. Знання кібербезпеки є надзвичайно важливими і для викладачів та адміністраторів навчальних закладів. Вони допомагають захистити освітні установи від кіберзагроз, таких як атаки на сервери, бази даних та інші важливі ресурси. Це забезпечує безперебійну роботу закладів освіти, захищає конфіденційну інформацію про студентів і персонал та підтримує високий рівень довіри до навчальних закладів. Обізнаність про кіберзагрози та методи захисту від них допомагає зменшити ймовірність успішних атак. Користувачі, які мають знання про потенційні загрози, можуть швидко розпізнати їх та реагувати належним чином, що значно знижує ризик втрати даних або порушення роботи систем. Це сприяє загальному підвищенню рівня кібербезпеки як на індивідуальному рівні, так і на рівні організацій.

Підводячи підсумок всього вищесказаного, навчання з кібербезпеки в 2024 році стане не тільки необхідністю, але й вигідною інвестицією як для організацій, так і для окремих професіоналів. Зростаюча кількість і складність кібератак, поява нових технологій, таких як синтетичний штучний інтелект, і потреба в інноваційних стратегіях безпеки підкреслюють важливість цієї сфери. Експерти з кібербезпеки стають незамінними для організацій, які хочуть захистити свої дані та інфраструктуру. Вивчення кібербезпеки відкриває багато кар’єрних можливостей у різних секторах економіки, включаючи фінансові установи, організації охорони здоров’я, державні структури та багато інших. Це дозволяє фахівцям адаптуватися до конкретних вимог різних галузей і отримувати конкурентоспроможну зарплату. Сучасні загрози, такі як використання штучного інтелекту у фішингових атаках, вимагають від експертів постійного вдосконалення своїх знань і навичок. Все більш популярна архітектура Zero Trust вимагає глибокого розуміння принципів кібербезпеки та здатності виконувати складні стратегії захисту. Організації, які інвестують у навчання своїх співробітників, отримають вигоду у вигляді підвищеної безпеки та захисту від кібератак. Навчання з кібербезпеки також включає вивчення нових технологій, таких як блокчейн і квантові обчислення,

які можуть як покращити безпеку, так і створити нові загрози. Розуміння цих технологій дозволяє фахівцям залишатися на передньому плані боротьби з кіберзлочинністю та ефективно захищати організації від сучасних загроз. Враховуючи всі ці фактори, навчання з кібербезпеки є не тільки корисним, але й необхідним, щоб залишатися в безпеці в сучасному цифровому світі. Це інвестиція, яка окупається завдяки підвищенню стійкості організації до кібератак і можливостям кар'єрного зростання для професіоналів. Зі стрімким розвитком технологій і зростанням кіберзагроз навчання з кібербезпеки залишатиметься ключовим чинником успіху в будь-якій сфері в 2024 році і наступних також.

Список використаних джерел

1. Slovo i Dilo. Названа кількість кібератак в Україні за минулий рік. Слово і Діло. URL: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik
2. Прогноз кіберзагроз 2024 - H-X Technologies. H-X Technologies. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua
3. Five Cybersecurity Predictions for 2024. SecurityWeek. URL: https://www.securityweek.com/five-cybersecurity-predictions-for-2024/
4. Учасники проектів Вікімедіа. DoS-атака – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/DoS-атака