УДК 65: 351.86, 004.5, 351.865

Л.В. Мазник [1]*, З.П. Двуліт [2]**
ORCID: [1]0000-0002-5387-7442, [2]0000-0002-2157-1422
*Національний університет харчових технологій
Національний університет "Львівська політехніка"

УПРАВЛІННЯ ДІЯЛЬНІСТЮ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

https://doi.org/

Стаття присвячена дослідженню управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення. В дослідженні наголошується, що кібербезпека вимагає технічної експертизи, розуміння загроз та ризиків, їх виявлення та запобігання кібератакам, дотримання етичних та правових стандартів. Зокрема, ідентифіковані ключові етичні аспекти, з якими стикаються фахівці з кібербезпеки. Дослідження підкреслює важливість навчання, вдосконалення навичок, диференціацію між особистісними навичками (soft skills) і адаптивними навичками (transferable skills), виявлення та реагування на кіберагресію та актуальність міжнародного співробітництва. Такий підхід сприяє забезпеченню безпеки організацій у сучасному інформаційному середовищі. Новизною дослідження є визначення змісту діяльності фахівців з кібербезпеки відповідно до основних концепцій кібербезпеки в умовах повномасштабної війни. Саме для таких фахівців визначена специфіка відповідних навичок в умовах впливу військових кіберризиків та інтенсифікації кіберзазагроз.

Ключові слова: кібербезпека, концепції кібербезпеки, кіберфахівці, особистісні навички, адаптивні навички, управління, кіберзагрози, повномасштабне вторгнення.

Постановка проблеми

З початку повномасштабного вторгнення росії на територію України, зафіксовано понад 3 тисячі кіберінцидентів та значна кількість кібератак. Заступник голови державної служби спеціального зв'язку та захисту інформації України, який відповідає за цифровий розвиток, цифрову трансформацію та цифровізацію, пояснює, що кібератаки стали повсякденною реальністю через те, що Україна переживає повноцінну кібервійну, що є першою в світі [1]. Ця війна розпочалася 9 років тому після анексії Криму та окупації східної частини Донбасу. З 14 січня 2022 року всі установи постійно піддаються кібератакам, але експерти ефективно протистоять цим атакам. За його словами, запобігти кібератакам можливо за допомогою комплексу заходів, включаючи використання спеціальних засобів кіберзахисту, співпрацю між ключовими суб'єктами в галузі кібербезпеки, негайну реакцію на кіберінциденти, дотримання правил кібергігієни та рекомендацій від експертів у галузі кібербезпеки.

Зокрема, за даними Державної служби спеціального зв'язку та захисту інформації [2], було зафіксовано декілька спроб кібератаки з використанням електронних листів на тему «рахунків/оплати». Звичайна мета зловмисника полягає у тому, щоб отримати доступ до бухгалтерських даних, які використовуються для фінансової діяльності, а також у отриманні персональних даних (тобто логін, пароль, ключ/сертифікат) та їх використанні для проведення несанкціонованих платежів.

Отже, виникла необхідність розробки та впровадження ефективної системи управління фахівцями з кібербезпеки в умовах постійних кібератак та повномасштабного кібервторгнення і зростаючих загроз національній кіберінфраструктурі.

Актуальність дослідження.

Факторами, які актуалізують роль фахівців з кібербезпеки загалом, є розширення світового доступу до Інтернету та зростання популярності нових цифрових технологій. Наявність різноманітних фахівців з безпеки з унікальним досвідом, перспективами та поглядами вкрай важлива для захисту та обслуговування різних ринків. Національна система кібербезпеки України має наступні завдання [3]:

1. Зміцнення передньої лінії оборони від кіберзагроз шляхом підвищення загальної обізнаності щодо інцидентів, уразливостей та загроз у державних установах, об'єктах критичної інфраструктури та громадському сегменті.

2. Запобігання вторгненням шляхом обміну інформацією та впровадження контрзаходів для зменшення поточних вразливостей.

3. Захист від повного спектру загроз шляхом підвищення контррозвідувальних та розвідувальних можливостей.

4. Зміцнення кібербезпеки через освітянські, медійні та громадські ініціативи.

5. Підтримка та сприяння проведенню кібернавчань, наукових досліджень та розробок в галузі кібербезпеки.

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» [4] та відповідними рішеннями Ради Національної безпеки та оборони України, ключовими компонентами Національної системи кібербезпеки є організаційно-технічна модель та відповідні їй елементи, включаючи національні центри управління кібербезпекою, галузеві центри управління безпекою (SOC, Security Operations Centers), центри реагування на кіберзагрози (CERT, Computer Emergency Response Team) та приватні структури.

Актуальність теми управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення стає особливо важливою в сучасному світі, оскільки кіберзагрози набувають все більшого масштабу та складності. Україна, перебуваючи в епіцентрі геополітичних подій, стикається з непередбачуваними викликами у цій сфері. Зростаюча кількість кіберінцидентів та кібератак, які спостерігаються на території України, свідчить про актуальність проблеми.

Забезпечення ефективного управління діяльністю фахівців з кібербезпеки стає критично важливим завданням для забезпечення національної безпеки та захисту критичної інфраструктури. У цьому контексті, розробка та впровадження національної системи кібербезпеки набувають найвищої актуальності, оскільки вона є ключовим інструментом для координації та ефективного управління заходами з кіберзахисту.

Крім того, зростаюча кількість кіберзагроз, включаючи кібершпигунство, кіберсаботаж і кібертероризм, підкреслює необхідність постійного оновлення стратегій та методів управління діяльністю фахівців з кібербезпеки. Актуальність теми підкреслюється також тим, що кіберзагрози не обмежуються однією країною і можуть мати глобальний вплив.

Отже, управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення залишається актуальною та нагальною проблемою для України, яка стикається зі зростаючими кіберзагрозами та потребує ефективних заходів для захисту національної кіберінфраструктури та інформаційних ресурсів.

Формулювання мети і завдань.

Мета дослідження полягає у визначенні змісту діяльності фахівців з кібербезпеки відповідно до основних концепцій кібербезпеки. До основних завдань дослідження належать: проаналізувати

відповідність українського законодавства в сфері кібербезпеки сучасним реаліям; здійснити класифікацію навичок в умовах впливу військових кіберризиків та інтенсифікації кіберзазагроз; обґрунтувати підходи до диференціації soft skills і transferable skills; провести порівняльний аналіз інтенсивності та динаміки кіберцілей; ідентифікувати ключові етичні аспекти, з якими стикаються фахівці з кібербезпеки.

Аналіз останніх досліджень і публікацій.

Аналіз останніх досліджень і публікацій в галузі кібербезпеки підтверджує драматичне зростання кіберзлочинності, що становить серйозну загрозу для суспільства і бізнесу [5]. За цими даними:

1. Кіберзлочинність зросла на 600% під час пандемії COVID-19, що свідчить про зростаючий обсяг кібератак у зв'язку зі змінами в робочому середовищі.

2. Прогнозується, що до 2025 року світові збитки від кіберзлочинності досягнуть 10,5 трильйонів доларів США щорічно, відзначаючи значне збільшення витрат.

3. Глобальні щорічні витрати на боротьбу з кіберзлочинністю оцінюються в 6 трильйонів доларів США на рік, що ставить цю проблему в центр уваги.

4. Вартість кіберзлочинності вже становить 1% світового ВВП, що свідчить про її вплив на світову економіку.

5. Середня вартість атаки зловмисного програмного забезпечення для компаній складає понад 2,5 мільйона доларів, включаючи витрати на відновлення.

6. У 2021 році відзначено 57-кратне зростання руйнівності програмного забезпечення-вимагача порівняно з 2015 роком, що свідчить про еволюцію загроз.

7. Велика кількість малих і середніх підприємств у США (понад 66%) стали жертвами кібератак у 2018-2020 роках, що вказує на розповсюдження загрози на різні сектори економіки.

8. Витоки даних для малих підприємств можуть призвести до серйозних фінансових втрат, що ставить питання про необхідність вдосконалення кіберзахисту.

9. Валові витрати на 56абл.56ція56ки зросли на 22,7% у 2021 році, свідчачи про збільшену увагу до цієї проблеми.

10. Річна кількість порушень безпеки організацій підприємств зросла на 27,4%, що вказує на посилення активності зловмисників.

11. Час відновлення після інсайдерських атак і атак програм-вимагачів є значною проблемою, вимагаючи серйозних ресурсів.

12. Розширення цінових моделей та доступність інструментів для зловмисників призводить до зростання кіберзлочинності.

Усі ці факти підкреслюють актуальність та серйозність проблеми кібербезпеки, а також необхідність надійного нормативного регулювання і заходів з забезпечення безпеки в цій галузі.

Останні дослідження в галузі кібербезпеки фокусуються на вивченні наступних проблем:

1. Дискусійність застосування штучного інтелекту (ШІ) та машинного навчання (МН). Застосування ШІ і МН у кібербезпеці стає все більш поширеним. Ці технології використовуються для виявлення загроз, аналізу підозрілих активностей та навіть автоматичного реагування на кібератаки.

2. Активізація та поширення кіберзагроз в Інтернеті речей (IoT). Зі зростанням кількості підключених до Інтернету пристроїв, виникає більше можливостей для кіберзловмисників. Дослідження спрямовані на розробку методів захисту великих мереж IoT.

3. Поява кібератак з державним замовленням. Така тенденція вказує на те, що деякі держави використовують кібератаки як інструмент геополітичного впливу. Дослідження зосереджуються на виявленні та аналізі таких атак.

4. Складність у виявленні загроз з боку внутрішніх джерел. Внутрішні загрози, такі як кіберзловмисники, які працюють усередині організацій, стають все серйознішою проблемою. Дослідження спрямовані на виявлення та запобігання таким загрозам.

5. Зростання різноманіття кіберзлочинності та кібермисливства. Такі проблеми досліджують з позицій психології та мотивації кіберзловмисників, щоб краще розуміти їхню діяльність та розробляти стратегії захисту.

6. Налагодження міжнародної співпраці. Оскільки кіберзагрози не мають кордонів, дослідники активно співпрацюють на міжнародному рівні для обміну інформацією та розробки спільних підходів до кібербезпеки.

Одним із суттєвих викликів, які стоять перед національною системою кібербезпеки України, є повномасштабне вторгнення росії, яка веде агресивні дії, включаючи кібератаки. Ця загроза надзвичайно актуальна та серйозна, і відповідно до пункту 37 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року під назвою «Про План реалізації Стратегії кібербезпеки України» і введеного в дію Указом Президента України від 1 лютого 2022 року № 37, Кабінет Міністрів України прийняв рішення затвердити Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі [6]. Також у цьому рішенні рекомендовано враховувати вимоги Порядку під час проведення заходів із забезпечення кібербезпеки.

Виклад основного матеріалу.

Російські державні хакерські групи ведуть активну багаторівневу та багатовекторну кампанію з метою отримати важливу перевагу в кіберпросторі в умовах війни, і в цьому процесі часто досягають різних результатів. Ця кампанія базується на: фокусуванні уваги різних груп населення світу на Україну з маніпулятивною метою; стрімкому збільшення кількості руйнівних атак на українські державні, військові та цивільні об'єкти; значному зростанні спроб спірфішингу. З англійської мови spear-phishing – це вид кібератаки, який полягає в тому, що зловмисники намагаються здійснити шахрайську дію шляхом надсилання спеціально спроектованих, схожих на легітимні повідомлення, які надходять електронною поштою або через інші комунікаційні канали з метою отримання від користувача конфіденційної інформації шахрайськими методами. До такої інформації відносять паролі користувачів, банківські реквізити або інші особисті дані.

Однак, відмінність спірфішингу від звичайного 57абл.57ц полягає в тому, що в атаках спірфішингу зловмисники часто націлюються на конкретну особу або організацію, використовуючи інформацію про них, яку вони знаходять в публічних джерелах або отримують через різні кібершпигунські методи. Це робить спірфішинг більш цілеспрямованим і небезпечним видом атаки, оскільки зловмисники можуть набагато легше переконати потенційну жертву у легітимності повідомлення або запиту. Такий спірфішинг спрямований на збільшення обсягу кібероперацій, спрямованих на досягнення різних цілей агресора. Зокрема, зловмисники використовують хакерські методи для створення можливості витоку чутливої інформації з метою підтримки певного сценарію. Російські урядові хакери посилили кібероперації, починаючи з 2021 року, ще перед повномасштабним вторгненням в Україну. У 2022 році ворог збільшив обсяг нападів на користувачів в Україні на 250% порівняно з 2020 роком (рис.1).

З 2021 по 2022 рік цілями росії були 150 військових і урядових установ з доменами gov.ua та mil.gov.ua. Цілі включали військові й дипломатичні організації, також урядові агенції, які управляють критичною інфраструктурою, державними послугами та управління надзвичайними ситуаціями.

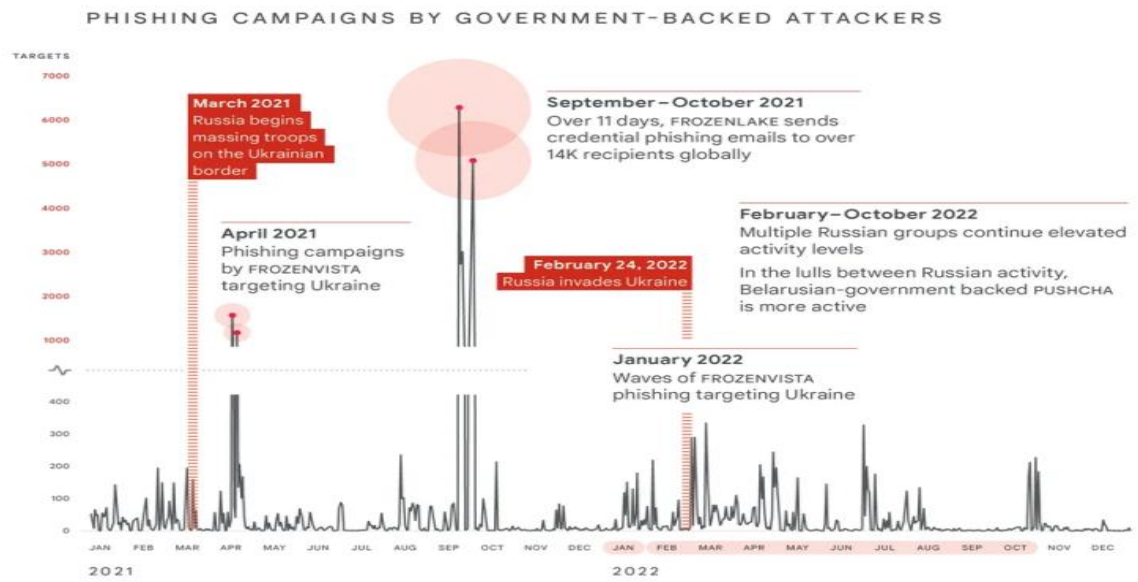

Рис.1. Фішингові кампанії, здійснювані з використанням підтримки уряду
Джерело: [7]

Топ-10 цілями були – Міністерство оборони, Міністерство закордонних справ, Національне агентство з питань державної служби, Державне агентство з водних ресурсів, Державна прикордонна служба, Служба безпеки України, Укрзалізниця, Дніпровська міська рада, Верховна Рада України (Парламент), Міністерство юстицій.

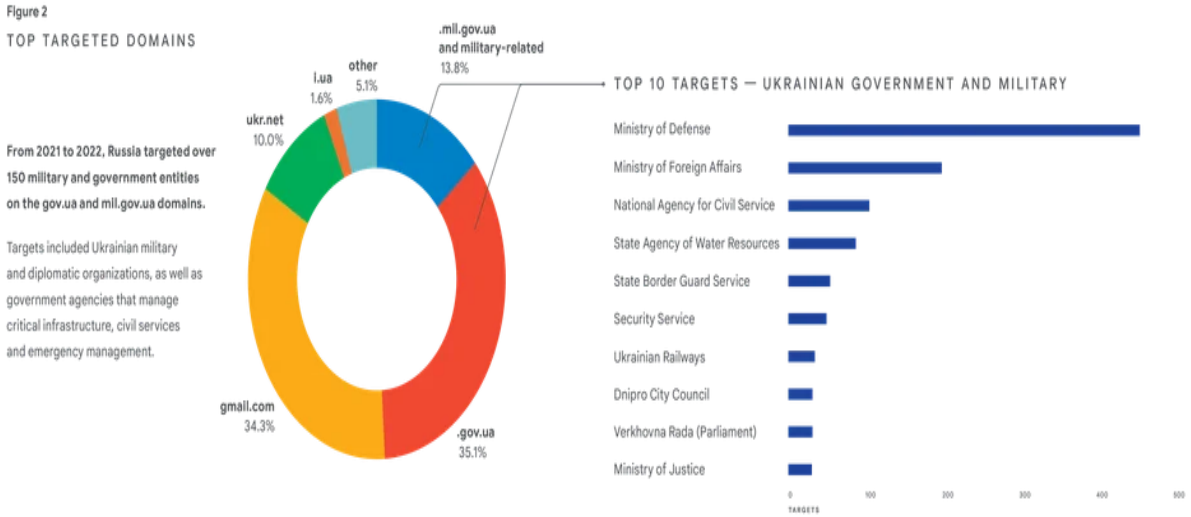

Рис.2. Основні цілі російських хакерів
Джерело: [7]

У 2022 році російські урядові хакери направили свою увагу на користувачів в Україні більше, ніж на користувачів будь-якої іншої країни. Ці атаки конкретно націлені на українські урядові і військові структури, об'єкти критичної інфраструктури, комунальні служби, медіа та інформаційний простір, великі компанії тощо.

Під час активізації російських урядових хакерів у 2022 році збільшилася загроза для України в кіберпросторі. Така загроза створила необхідність для фахівців з кібербезпеки в Україні вдоскона-

лити свої навички та засоби для захисту організацій від кіберзагроз. Для ефективного захисту важливо розробити чіткий зміст діяльності фахівців з кібербезпеки, який відповідав би основним концепціям безпеки в кіберпросторі та враховував специфічність сучасних кіберзагроз. Такий зміст дільності стане надійним щитом для організацій і допоможе відповідати вимогам безпеки та регуляцій у складних умовах загострення кіберконфлікту.

Для реалізації мети дослідження визначений зміст діяльності фахівців з кібербезпеки у відповідності до основних концепцій кібербезпеки. Формулювання змісту діяльності допоможе фахівцям з кібербезпеки забезпечити надійний захист організації та відповідність вимогам безпеки та 59абл.59ція. Запропонована табл.1 надає загальний огляд ключових концепцій у галузі кібербезпеки та розкриває зміст діяльності фахівця з кібербезпеки для реалізації кожної з цих концепцій. Кожен стовпчик містить короткий опис концепції, її значення та обов'язки фахівця з кібербезпеки, які пов'язані із цією концепцією. Ця інформація допомагає розуміти важливі аспекти та завдання, які входять до компетенції фахівців з кібербезпеки при забезпеченні безпеки організації та її активів. Безпека в інформаційному просторі є надзвичайно важливою, і розуміння цих концепцій допомагає створити міцні та надійні заходи для захисту від кіберзагроз.

Таблиця 1

Ключові концепції кібербезпеки та завдання фахівців з кібербезпеки

Концепція кібербезпеки	Зміст концепції	Зміст діяльності фахівця з кібербезпеки для реалізації цієї концепції
1	2	3
Відповідність вимогам (Compliance)	Це процес відповідності внутрішнім стандартам та зовнішнім регуляціям, який дозволяє організаціям уникати штрафів та порушень безпеки	Встановлення внутрішніх стандартів та процедур відповідно до зовнішніх регуляцій. Перевірка та забезпечення дотримання цих стандартів та регуляцій в організації. Проведення регулярних аудитів та оцінок відповідності.
Засоби безпеки (Security controls)	Це засоби захисту, призначені для зменшення певних ризиків безпеки. Вони використовуються разом із системами безпеки для встановлення надійної безпеки	Вибір, впровадження та конфігурація відповідних засобів захисту. Моніторинг та управління цими засобами для забезпечення ефективності та надійності захисту.
Стан безпеки (Security posture)	Це здатність організації керувати захистом критично важливих активів і даних і реагувати на зміни. Сильна безпека веде до зниження ризику для організації	Оцінка поточного стану безпеки організації та ідентифікація можливих вразливостей. Розробка та впровадження стратегій та заходів для покращення стану безпеки.
Загроза (Threat actor) або «зловмисний атакувальник»	Це будь-яка особа або група, яка становить ризик для безпеки. Цей ризик може стосуватися комп'ютерів, програм, мереж і даних	Аналіз і вивчення потенційних загроз та зловмисників. Розробка та впровадження заходів для запобігання атакам з боку загроз

Продовження табл. 1

1	2	3
Внутрішня загроза (Internal threat)	Це поточний або колишній співробітник, зовнішній постачальник або довірена сторона, яка становить ризик для безпеки. Іноді внутрішня загроза є випадковою. Наприклад, співробітник, який випадково «клікає» по посиланню у шкідливому електронному листі, вважається випадковою загрозою. В інших випадках внутрішній загрозливий актор навмисно займається ризикованою діяльністю, такою як несанкціонований доступ до даних	Моніторинг діяльності співробітників та інших довірених осіб. Розвиток систем для виявлення та запобігання внутрішнім загрозам.
Мережева безпека (Network security)	Це практика забезпечення безпеки інфраструктури мережі організації від несанкціонованого доступу. Це включає дані, сервіси, системи та пристрої, що зберігаються в мережі організації	Конфігурація та підтримка інфраструктури мережевої безпеки, включаючи мережеві пристрої та захист мережевого трафіку. Виявлення та реагування на мережеві загрози та інциденти.
Безпека хмарних сервісів (Cloud security)	Це процес забезпечення належної конфігурації активів, що зберігаються в хмарі, і обмеження доступу до цих активів для авторизованих користувачів. Хмара - це мережа, що складається з набору серверів або комп'ютерів, що зберігають ресурси та дані в віддалених фізичних розташуваннях, відомих як центри обробки даних, і до яких можна отримати доступ через Інтернет. Безпека хмарних сервісів - це зростаюче підполе кібербезпеки, спеціально спрямоване на захист даних, програм та інфраструктури в хмарі	Забезпечення належної конфігурації та безпеки активів в хмарі. Моніторинг та контроль доступу до хмарних ресурсів та даних.
Програмування	Це процес створення конкретного набору інструкцій для виконання завдань комп'ютером. Ці завдання можуть включати: автоматизацію повторюваних завдань (наприклад, пошук списку шкідливих доменів), перегляд веб-трафіку, сповіщення про підозрілу діяльність.	Розробка та впровадження програмних рішень для автоматизації процесів моніторингу та виявлення загроз. Розробка програм для виявлення та аналізу підозрілої діяльності.

Реалізація цієї діяльності повинна бути здійснена та удосконалена на основі відповідних технічних навичок (hard skills) та, так званих, адаптивних навичок (transferable skills) як частини soft skills. Soft skills і transferable skills є важливими для фахівців з кібербезпеки, але вони мають свої відмінності і ролі в цій галузі. Основні відмінності між ними представлені в табл. 2.

Таблиця 2

Порівняння особистісних (soft skills) та адаптивних (transferable skills) навичок для фахівців з кібербезпеки

Аспекти навичок у сфері кібербезпеки	Особистісні навички (soft skills)	Адаптивні навички (transferable skills)
Природа навичок	Це навички, пов'язані з особистісним розвитком і міжособистісними відносинами. Вони включають в себе такі аспекти, як комунікація, лідерство, співпраця, толерантність тощо.	Це навички, які можна використовувати у різних галузях і різних ролях. Вони включають аналітичні навички, управлінські здібності, рішення, вміння працювати в команді і багато інших.
Застосування в кібербезпеці	Soft skills, такі як комунікація і лідерство, важливі для спілкування з іншими фахівцями з кібербезпеки, клієнтами і стейкхолдерами. Вони можуть допомогти вирішувати конфлікти та сприяють побудові довіри у важливих ситуаціях.	Transferable skills, такі як аналітичні навички і управління проектами, можуть бути застосовані безпосередньо в аналізі кіберзагроз, розробці стратегій кібербезпеки і управлінні проектами кібербезпеки.
Типові завдання	Вони допомагають у вирішенні конфліктів, побудові співпраці та взаємодії з іншими фахівцями та стейкхолдерами, що може виникати в ході вирішення кіберзагроз і інцидентів.	Ці навички допомагають у виконанні конкретних завдань, таких як аналіз логів, виявлення вразливостей, створення політик безпеки тощо.
Тривалість навчання і розвитку	Зазвичай, soft skills розвиваються протягом тривалого часу і можуть вимагати більшого зусилля для вдосконалення.	Transferable skills можуть бути набуті швидше, і їх можна швидко адаптувати до потреб у сфері кібербезпеки.
Важливість у сфері кібербезпеки	Хоч soft skills важливі, вони часто вважаються менш пріоритетними, ніж технічні навички, але все ж є необхідними для успіху у галузі кібербезпеки.	Transferable skills є критично важливими, оскільки вони допомагають фахівцям з кібербезпеки адаптуватися до змінних обставин і ефективно вирішувати різні завдання.

Враховуючи ці відмінності, успішний фахівець з кібербезпеки повинен розвивати і об'єднувати обидві категорії навичок для досягнення максимальної ефективності в цій галузі. Для фахівців у галузі кібербезпеки важливо мати різноманітний набір навичок та якостей, які поєднують в собі технічні, міжособистісні та аналітичні аспекти. Усе це сприяє успішній роботі та вирішенню завдань у цій складній галузі.

1. Технічні навички: технічна експертиза є фундаментальною для фахівців з кібербезпеки. Вони повинні володіти глибоким розумінням технічних аспектів мереж, систем та програмного забезпечення, а також мати навички виявлення та виправлення уразливостей.

2. Міжособистісні навички: комунікація та співпраця грають ключову роль у кібербезпеці. Фахівці повинні бути здатні ефективно спілкуватися з іншими членами команди, взаємодіяти з клієнтами та робити узгоджену роботу. Емпатія та дружелюбність допомагають побудувати довіру в професійних відносинах.

3. Аналітичні навички: фахівці з кібербезпеки повинні мати аналітичний розум та здатність до логічного мислення. Вони аналізують дані про потенційні загрози та розробляють стратегії для їхнього виявлення та запобігання.

4. Мислення кіберзлочинця: для ефективного захисту системи важливо вміти думати як кіберзлочинець. Тобто, передбачати можливі шляхи атак та зразки поведінки зловмисників. Це допомагає виявляти слабкі місця в існуючих системах та запобігати атакам.

5. Інтуїція та рефлексія: у кібербезпеці часто потрібно швидко приймати рішення в ситуаціях, де кожна секунда має значення. Інтуїція допомагає фахівцям швидко виявляти загрози та реагувати на них. Рефлексія важлива для подальшого вдосконалення процесів та стратегій.

6. Життєвий досвід: досвід в інших сферах життя може бути корисним для фахівців з кібербезпеки. Він додає глибини їхньому розумінню загроз та робить їх більш креативними в пошуку рішень.

Таким чином, фахівці з кібербезпеки повинні поєднувати різні аспекти навичок та якостей для успішної роботи у цій динамічній галузі.

Фахівці з кібербезпеки в сучасному світі мають завдання вирішувати не лише технічні проблеми, а й враховувати складну етичну складову своєї діяльності. Ця галузь зосереджена на захисті від кіберзагроз, але разом з тим, вона впливає на приватність, безпеку, та права користувачів і організацій. Тому фахівцям з кібербезпеки необхідно мати не лише технічні навички, але й етичну свідомість, щоб уникнути порушень і захищати цінності індивідів і суспільства в цифровому просторі. Таким чином, вони повинні поєднувати різні аспекти навичок та якостей для успішної роботи у цій критично важливій галузі.

Отже, у сфері кібербезпеки існує ряд етичних питань, оскільки ця галузь має значний вплив на приватність, безпеку та права користувачів і організацій. Нижче наведено деякі ключові етичні аспекти, з якими стикаються фахівці з кібербезпеки:

1. Хакерські атаки та вторгнення. Виникають етичні питання стосовно дій хакерів, які зламують системи та комп'ютери без дозволу. Такі атаки можуть завдавати шкоду користувачам, компаніям та організаціям.

2. Збирання та зберігання персональних даних. Збирання та зберігання великих обсягів персональних даних створюють питання щодо приватності та можливого зловживання цими даними.

3. Масовий контроль. Уряди та інші організації можуть використовувати кібербезпеку для масового нагляду за громадянами, що порушує права на приватність.

4. Створення та використання кіберзброї. Розробка кіберзброї, такої як шкідливі програми, може викликати непередбачені ефекти та піднімати серйозні моральні та етичні питання.

5. Відповідальність за кібератаки. Визначення відповідальності за кібератаки та виявлення кіберзлочинців може бути складним завданням, що вимагає об'єктивності та справедливості.

6. Етика управління інцидентами кібербезпеки. Управління інцидентами потребує етичних рішень, оскільки важливо враховувати права користувачів та співробітників, а також дотримуватися вимог законодавства.

7. Відповідальність виробників програмного забезпечення. Питання етики виникають щодо відповідальності виробників за недоліки в програмному забезпеченні, які можуть спричинити кіберінциденти.

8. Соціальна інженерія. Цей вид атак використовує маніпуляцію та обман для отримання доступу до системи або даних, що породжує питання щодо етичності обману та впливу на довіру.

9. Розвиток штучного інтелекту (ШІ) в кібербезпеці. Використання ШІ в кібербезпеці може ставити питання щодо етичності рішень, які приймаються автоматизованими системами.

10. Військовий вимір кібербезпеки. Використання кіберзброї та кібератак у військових конфліктах породжує складні етичні питання. Введення цього аспекту етики у сферу кібербезпеки набуло особливої актуальності після повномасштабного вторгнення Росії в Україну 24 лютого 2022 року. У цьому контексті, використання кіберзброї та кібератак стають необхідними складовими військової стратегії. Однак такі дії викликають серйозні етичні питання. Перше з них полягає в тому, як визначити легітимність цифрової війни та визнавати норми міжнародного гуманітарного права в цьому контексті. Спільнота міжнародних гравців повинна домовитися щодо етичних норм та стандартів, які

регулюватимуть використання кіберзброї у військових конфліктах. Друге питання стосується цілей та об'єктів кібератак. Фахівці з кібербезпеки мають розуміти, як визначити прийнятність атак на важливі інфраструктурні об'єкти та приватні системи у військовому контексті. Це вимагає від них не лише технічних знань, але й етичного розсуду, щоб уникнути непропорційного збитку та колатеральних збитків для цивільного населення. Третє питання стосується визначення відповідальності за кібератаки в рамках міжнародного права. Розслідування кіберконфліктів та визначення винних можуть виявитися складними завданнями, і вони також потребують етичного підходу та справедливості.

Військовий вимір кібербезпеки породжує складні етичні дилеми, і фахівцям з кібербезпеки доводиться розглядати їх з урахуванням моральних та етичних аспектів. Важливо розвивати етичні стандарти та розуміння в цій галузі, щоб забезпечити відповідальне використання кіберзброї та кібератак у військових конфліктах та зберегти гідність і справедливість в цифровому просторі.

Ці етичні аспекти стають важливими обговорюваними темами у галузі кібербезпеки, і фахівцям необхідно здійснювати свою роботу з дотриманням високих стандартів етики та справедливості. Етика в кібербезпеці є важливою, оскільки вона визначає правила та норми для відповідної поведінки в цій галузі та сприяє збереженню довіри та безпеки в кіберпросторі.

Висновки.

У дослідженні, присвяченому управлінню діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення, були розглянуті важливі аспекти цієї актуальної проблеми. Виходячи з аналізу змісту діяльності фахівців з кібербезпеки та їхніх основних концепцій було визначено, що в цій галузі наявні проблеми, які вимагають від фахівців специфічних навичок і знань. Зокрема, фахівці з кібербезпеки повинні мати технічну експертизу, розуміти загрози та ризики, вміти виявляти та відвертати кібератаки, а також дотримуватися етичних та правових стандартів. Крім того, важливою є здатність спілкуватися та працювати в команді, а також враховувати соціокультурні та правові особливості країни, в якій вони працюють.

У контексті повномасштабного вторгнення росії в Україну 24 лютого 2022 року, фахівцям з кібербезпеки доводиться стикатися з викликами надзвичайної складності. Вони повинні реагувати на агресивні російські кібератаки, які спрямовані на різні сфери, включаючи урядові структури, критичну інфраструктуру, медіа та інформаційний простір. Одночасно їм слід враховувати етичні аспекти і відповідально взаємодіяти з іншими органами та організаціями для забезпечення колективного кіберзахисту.

Зазначене дослідження підкреслює важливість розвитку комплексного підходу до управління діяльністю фахівців з кібербезпеки в умовах вторгнення. Для цього необхідно забезпечити навчання та підвищення кваліфікації фахівців, створити ефективні механізми виявлення та реагування на кіберагресію, а також зміцнити міжнародну співпрацю у сфері кібербезпеки. Завдяки цим заходам фахівці з кібербезпеки матимуть можливість ефективно захищати інтереси своїх організацій і держави в умовах посиленої кіберзагрози, забезпечуючи безпеку, приватність і права користувачів. Такий підхід сприятиме створенню більш стійкого та безпечного інформаційного середовища, яке є важливим чинником в сучасному світі.

З врахуванням ключових концепцій у галузі кібербезпеки запропоновано зміст діяльності фахівця з кібербезпеки для реалізації кожної з цих концепцій, що є важливим внеском у розуміння комплексного підходу до кіберзахисту та вирішення завдань, пов'язаних з управлінням фахівцями з кібербезпеки.

У статті наведена порівняльна характеристика soft skills та transferable skills для фахівців з кібербезпеки з виокремленням ключових вмінь та якості, які є важливими в цій галузі, щоб виявляти їх взаємозв'язок та роль у успішній роботі фахівця. Це допомагає розробити більш ефективні стратегії підготовки та розвитку фахівців з кібербезпеки, сприяючи підвищенню їхньої професійної компетентності та відповідності сучасним вимогам безпеки.

Проведене дослідження сприятиме покращенню якості управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення акцентуючи важливість поєднання технічних (hard skills) та особистісних (soft skills) навичок для забезпечення надійності та ефективності кіберзахисту.

Перспективи подальших досліджень.

Подальші дослідження можуть спрямовуватися на розвиток стратегій кризового управління та забезпечення ефективного виявлення та відповіді на кібератаки в умовах повномасштабного вторгнення, з урахуванням управління діяльністю фахівців з кібербезпеки.

Список літератури

1. У 2022 році в Україні зареєстрували 2194 кіберінциденти. 2023. URL: https://suspilne.media/397220-u-2022-roci-v-ukraini-zareestruvali-2194-kiberincidenti-derzspeczvazku/.

2. Кіберзлочинці атакують поштові скриньки українців з темою «рахунки/оплати». 2023. URL: https://www.unn.com.ua/uk/news/2038596-kiberzlochintsi-atakuyut-poshtovi-skrinki-ukrayintsiv-z-temoyu-rakhunki-oplati.

3. Україна 2030E — країна з розвинутою цифровою економікою. 2023. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html.

4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakononline.com.ua/documents/show/377007___696128.

5. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2023. 2023. URL: https://purplesec.us/resources/cyber-security-statistics/#Cybercrime.

6. Постанова Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 4 квітня 2023 р. № 299. 2023. URL: https://zakononline.com.ua/documents/show/517068___737550.

7. Fog of war: how the Ukraine conflict transformed the cyber threat landscape. 2023. URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

References

1. Reshetilov H. O. (2022). Finansuvannia tsyrkuliarnoi ekonomiky: yevropeiskyi pohliad [Financing the circular economy: a European perspective]. *Modern Economics*, No. 32, 84–91. DOI: https://doi.org/10.31521/modecon.V32(2022)-11.

2. Nahara M. B. (2022). Biznes-modeli tsyrkuliarnoi ekonomiky: kontseptualnyi dyskus [Circular economy business models: a conceptual discussion]. *Odesa National University Herald*, Vol. 7, No. 1(91), 13–17. URL: https://web.archive.org/web/20220409211527id_/http://www.visnyk-onu.od.ua/journal/2022_27_1/4.pdf DOI: https://doi.org/10.32782/2304-0920/1-91-2

3. Varchenko O., Artimonova I., Herasymenko I. (2020). Formuvannia systemy upravlinnia rezultatyvnistiu marketynhovoi diialnosti ahrarnykh pidpryiemstv na osnovi systemy zbalansovanykh pokaznykiv [Formation of a management system for the effectiveness of marketing activities of agrarian enterprises based on a system of balanced indicators]. *The economic discourse*, Vol. 2, 95–108. DOI: https://doi.org/10.36742/2410-0919-2020-2-10.

4. Kuzmin O. Ye., Melnyk O. H. (2007). Osnovy menedzhmentu [Basics of management]. K.: Akademvydav, 464 p.

5. Zakharchyn H. M., Andriichuk Yu. A. (2012). Planuvannia innovatsiinoi diialnosti: alternatyvy i etapy [Planning of innovative activities: alternatives and stages]. *Actual problems of the economics*, No. 5, 169–175.

6. Yatsenko O., Shvydanenko O., Shvydanenko H. (2022). Tsyrkuliarna ekonomika yak osnova zabezpechennia staloho rozvytku krainy v konteksti yevrointehratsii [Circular economy as a basis for ensuring sustainable development of the country in the context of European integration]. *Economics and Region*, Vol 4 (87), 150–167. DOI: https://doi.org/10.26906/EiR.2022.4(87).2794.

7. Kvasnii L. H., Popivniak O. M., Shcherban O. Ya. (2015). Stratehichne i taktychne planuvannia diialnosti pidpryiemstva yak osnovni skladovi mekhanizmu zabezpechennia yoho ekonomichnoi bezpeky [Strategic and tactical

planning of the enterprise's activities as the main components of the mechanism for ensuring its economic security]. *Scientific Bulletin of Mykolaiv National University named after V.O. Sukhomlynskyi. Economic sciences*, No. 1, 48–53.

L. V. Maznyk*, Z.P. Dvulit**
National University of Food Technologies
**Lviv Polytechnic National University

MANAGING THE ACTIVITIES OF CYBERSECURITY PROFESSIONALS IN THE CONTEXT OF FULL-SCALE INTRUSION

In this study dedicated to the management of cybersecurity professionals in the context of full-scale intrusion, significant aspects of this pressing issue have been examined. Drawing from an analysis of the content of cybersecurity professionals' activities and their core concepts, it has been identified that this field encompasses various facets requiring diverse skills and knowledge from these experts. Specifically, cybersecurity experts must possess technical expertise, understand threats and risks, detect and thwart cyberattacks, and adhere to ethical and legal standards. Additionally, the ability to communicate and collaborate within a team, while considering socio-cultural and legal peculiarities of the country they operate in, is vital. In the context of full-scale intrusion, such as russia's invasion of Ukraine in 2022, cybersecurity professionals face challenges of extraordinary complexity. They must respond to aggressive cyberattacks targeting various sectors, including governmental structures, critical infrastructure, media, and the information space. Simultaneously, they must consider ethical aspects and responsibly engage with other entities and organizations to ensure collective cyber defense.

This research underscores the importance of adopting a comprehensive approach to managing cybersecurity professionals in times of intrusion. To achieve this, it is essential to provide training and continuous skill enhancement, establish effective mechanisms for detecting and responding to cyber aggression, and strengthen international cooperation in the field of cybersecurity. Through these measures, cybersecurity professionals will have the capability to effectively safeguard the interests of their organizations and nations amidst heightened cyber threats, ensuring the security, privacy, and rights of users. Such an approach contributes to creating a more resilient and secure information environment, a critical factor in the modern world.

Furthermore, the article presents a comparative analysis of soft skills and transferable skills for cybersecurity professionals, highlighting key abilities and qualities crucial in this field. This analysis helps develop more effective strategies for training and developing cybersecurity experts, enhancing their professional competence to meet contemporary security demands. This analysis also promotes the improvement of managing cybersecurity professionals in the context of large-scale intrusion, emphasizing the importance of combining technical and interpersonal skills to ensure the reliability and effectiveness of cybersecurity.

Keywords: cybersecurity, conception of cybersecurity. Cybersecurity professionals, soft skills, transferable skills, management, cyber threats, full-scale intrusion