УДК 004.946.5.056:316.3(477)
DOI: 10.31866/2616-7654.10.2022.269495

КІБЕРБЕЗПЕКА ТА КІБЕРЗАХИСТ: ПИТАННЯ ПОРЯДКУ ДЕННОГО В УКРАЇНСЬКОМУ СУСПІЛЬСТВІ

Зоряна Свердлик,
кандидатка історичних наук, доцентка,
доцентка кафедри інформаційних технологій
Київського національного університету
культури і мистецтв
(Київ, Україна)
e-mail: zsverdlyk@gmail.com
ORCID: 0000-0002-2104-0920

Метою статті є аналіз понять «кібергігієна», «кібербезпека», «кіберзахист» та з'ясування ролі тих процесів, що тлумачаться цими термінами у сучасному житті людини; визначення головних досягнень в українському законодавстві щодо правового регулювання кібернетичної сфери; виокремлення ключових правил дотримання кібергігієни.

Методологія дослідження реалізована застосуванням наукових методів термінологічного аналізу при зіставленні дефініцій відповідних термінів; статистичного методу – для узагальнення кількісних показників, що характеризують підвищення зацікавленості закладів вищої освіти у підготовці фахівців із кібербезпеки; порівняння і узагальнення, що дозволили всебічно розкрити порушену у дослідженні проблему

Наукова новизна дослідження полягає у: наголошенні на важливості та необхідності співпраці українських організацій із закордонними партнерами у сфері захисту інформації, що міститься у кіберпросторі; виявленні та простеженні тенденцій щодо підвищення кібербезпеки зі сторони науки, освіти, державного управління.

Висновки. Розгляд питання забезпечення в Україні кіберзахисту інформації, кібербезпеки при користуванні мережею інтернет, кібергігієни показав, що українські фахівці зробили значний крок уперед у цих питаннях, і це підтверджується міжнародними статистичними даними.

Аналіз прийнятих останнім часом на національному рівні законодавчих, нормативно-правових актів і нормативних документів підтвердив тезу про те, що поступово українське законодавство з питань кібербезпеки переорієнтовується на світові тенденції та запозичує позитивний іноземний досвід. Однак існують і невирішені досі нагальні питання, серед яких ключовим є зведення понятійного апарату кібербезпеки до закріплених на законодавчому рівні тлумачень.

Важливе також питання подальшого поглиблення міжнародного співробітництва у питаннях кіберзахисту та кібербезпеки, створення спільних міждержавних платформ для обміну інформацією.

Не менш важливим є розвиток і розширення освітніх програм спеціальності 125 «Кібербезпека» у закладах вищої освіти України. Як показали результати дослідження, зацікавлення цією професією серед молоді останнім часом зростає.

Ключові слова: кібергігієна, кіберзахист, кібербезпека, мережа інтернет, спеціальність «Кібербезпека», кіберзагроза, закон, рекомендація.

ВСТУП

В умовах глобалізаційних процесів та епідемічних криз, що останніми роками з'явилися і активно поширюються світом, актуалізувалося використання комп'ютерних технологій в усіх сферах суспільного та приватного життя. Важко сьогодні уявити будь-яку сферу діяльності, де не використовувалися б гаджети. Вони покликані спростити професійну діяльність сучасної людини та зробити інформацію доступною. Однак разом із розвитком технологій виникла проблема захисту певних видів інформаційних ресурсів, як-от персональні дані особи, різноманітна конфіденційна інформація, бізнес-інформація тощо.

Активно вживаються у повсякденному житті такі терміни, як «кібергігієна», «кібербезпека», «кіберзахист». При цьому якщо для двох останніх понять в українському законодавстві існує чітке тлумачення, то різні дослідники визначають «кібергігієну» дещо відмінними характеристиками. Тому необхідно дослідити походження термінів та показати, який зміст вкладають науковці у ці поняття, що намагаються пояснити з їхньою допомогою. Зауважимо, що ці поняття увійшли до нашого лексикону нещодавно, але за короткий час стали актуальними та незамінними.

Метою статті є аналіз понять «кібергігієна», «кібербезпека», «кіберзахист» та з'ясування ролі тих процесів, що тлумачаться цими термінами у сучасному житті людини; визначення головних досягнень в українському законодавстві щодо правового регулювання кібернетичної сфери; виокремлення ключових правил дотримання кібергігієни.

ТЕОРЕТИЧНЕ ПІДҐРУНТЯ

Актуальним сьогодні є аналіз праць дослідників, що стосуються не лише проблем походження термінів, але й торкаються аспектів захисту кібернетичного простору держави, його убезпечення від внутрішніх і зовнішніх атак, вироблення принципів і засобів підтримання особистої та суспільної кібергігієни тощо. Так, І. Кочан у своєму дослідженні звернулася до питання збору та тлумачення слів із компонентом «кібер-» та дійшла висновку, що такі слова позначають абстрактні поняття, поняття культури, поняття спорту, поняття права і криміналу, комп'ютерні програми, поняття медицини, соматичні, військової справи, поняття освіти, елементи одягу, іграшки та ін. Авторка зауважує, що частина слів із «кібер-» не мають чітких визначень, тому їх поки що можна відносити лише до протермінів (Кочан, 2016, с. 283).

А. Головка аналізує головні проблеми української системи протидії кіберзагрозам на основі окремих конкретних прикладів (Головка, 2016) та бачить вирішення існуючих питань кількома шляхами, головним з яких є залучення до державних розробок систем захисту кіберпростору якомога більшого числа спеціалістів із інститутів громадянського суспільства.

Ю. Лісовська розглянула усі аспекти поняття «кібербезпека» та запропонувала власне розуміння поняття адміністративно-правового забезпечення кібербезпеки як комплексу превентивних дій економічного, політичного, юридичного, технологічного та організаційного характеру, спрямованих на попередження, виявлення і ліквідацію загроз інтересам особи, держави та суспільства в електронній сфері (Лісовська, 2019, с. 12).

О. Бакалінська та О. Бакалинський зосередили увагу на нормативно-правових аспектах організації та забезпечення кібернетичної безпеки держави і констатували, що сьогодні законодавче регулювання кіберзахисту в Україні перебуває на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту – пройдено (Бакалінська & Бакалинський, 2019, с. 100).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Останнім часом у пресі часто з'являються повідомлення про активізацію кібершахраїв, злам систем захисту не тільки відомих соціальних мереж чи окремих сторінок впливових світових діячів, але й офіційних онлайн-сервісів урядових органів, органів місцевого самоврядування тощо. Це підтверджує думку про те, що в Україні, як і в усьому світі, існує проблема захисту інформації та кіберпростору держави. З масовим розповсюдженням технології інтернету речей, переходом у хмарні сховища даних, формуванням обліку цифрових та криптовалют, криптобірж, електронних виборів і «розумних контрактів» для зниження небезпечних вразливостей треба ретельно захищати метадані від можливого викрадення унаслідок зловмисних атак. Сьогодні критично важливі інфраструктурні компанії відстають у підготовці своїх операційних можливостей для протистояння кібератакам. Це робить їх легкою здобиччю для політично мотивованих нападників. Такі рішення, як цифрові підписи та шифрування, доступні для надійних пристроїв ідентифікації, можуть допомогти вирішити цю проблему (Трофименко та ін., 2019, с. 155).

Ключовими інституціями, що відповідають за кібербезпеку в Україні, є Міністерство цифрової трансформації України (Мінцифра) і Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку).

Міністерство цифрової трансформації України було створено відповідно до Постанови Кабінету Міністрів України від 02 вересня 2019 р. № 829 «Деякі питання оптимізації системи центральних органів виконавчої влади». Зокрема, пункт 5 Постанови затвердив утворення Мінцифри шляхом реорганізації Державного агентства з питань електронного урядування ("Деякі питання оптимізації", 2019). У прийнятій Кабінетом Міністрів України Постанові від 18 вересня 2019 р. № 856 ("Питання Міністерства", 2019), окрім іншого, на Мінцифри було покладено обов'язки щодо участі у формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, захисту державних інформаційних ресурсів та інформації, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку.

Держспецзв'язку створена відповідно до Указу Президента України від 07 листопада 2005 р. № 1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів» (2005). Згодом, у 2006 р. було прийнято Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» ("Про Державну службу", 2006), відповідно до положень якого основними завданнями Служби стали кіберзахист, захист державних інформаційних ресурсів та інформації, протидія технічним розвідкам тощо. Останнім часом Служба активізувала діяльність у напрямі підвищення рівня кіберзахисту об'єктів інфраструктури. Так,

при Державному центрі кіберзахисту та протидії кіберзагрозам, що є складовою загальної структури Держспецзв'язку, функціонує підрозділ Computer response team of Ukraine (CERT-UA) – команда реагування на надзвичайні комп'ютерні події в Україні, основною метою якого є забезпечення захисту інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності; організація і проведення практичних семінарів із питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; взаємодія із правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки та ін. ("Про CERT-UA", б.р.). CERT-UA періодично публікує рекомендації, які стосуються безпеки поштового сервісу, із протидії загрозі інсайдера, усунення вразливостей, пов'язаних із некоректним налаштуванням DNS-серверів, із самостійного пошуку та ліквідації веб-шеллів тощо (Бакалінська & Бакалинський, 2019, с. 103).

Відповідно до результатів досліджень, проведених естонською Академією електронного урядування та висвітлених у новій редакції Національного індексу кібербезпеки за 2020 р., Україна посіла 25 місце серед 160 аналізованих країн. До уваги бралися такі параметри, як законодавство та освіта у сфері кібербезпеки, захист персональних даних та електронних послуг, реагування на кібератаки та кіберінциденти, боротьба із кіберзлочинністю ("Україна посіла 25 місце", 2020). Незважаючи на такий добрий результат, у нашій країні сьогодні ще є проблеми, вирішення яких стоїть на порядку денному. Насамперед мова йде про підсумки реалізації Стратегії кібербезпеки України періоду 2016–2021 рр., аналіз яких дозволив виокремити актуальні аспекти, що потребують вирішення. Це – недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була неконкретною, заплановані заходи не завжди корелювалися із визначеними завданнями. Реалізація зазначеної Стратегії була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення; не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства; розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично ("Про рішення Ради", 2021). Важливо також звернути увагу на наявну проблему розбіжностей у тлумаченні таких ключових понять, як «кібербезпека», «кібергігієна», «кіберзахист».

Кібергігієна – це термін, який використовується для захисних процедур вашої особистої та фінансової інформації під час використання комп'ютера чи мобільного пристрою. Хороша кібергігієна означає дотримання розумних щоденних практик щодо здоров'я та безпеки вашої інформації в інтернеті. Вона включає, але не обмежується цим, регулярне оновлення програмного забезпечення браузера, встановлення та підтримку програмного забезпечення для захисту, вибір надійних паролів, якими ніколи не ділиться, а також уникає загальнодоступного Wi-Fi для онлайн-банкінгу та інших фінансових операцій. Ідея полягає в тому, щоб заблокувати шахраїв і злодіїв ("Кібергігієна… Що це?" 2021). Натомість спеціалісти ESET (компанії-лідера із розробки програмного забезпечення захисту інформації

та робочих станцій) під кібергігієною розуміють «заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації» (Основні правила захисту даних). Зі свого боку, фахівці ITech (компанії, що займається комп'ютерним обладнанням та програмами) розглядають кібергігієну як термін, «який використовується для захисних процедур вашої особистої та фінансової інформації під час використання комп'ютера чи мобільного пристрою», коли «хороша кібергігієна означає дотримання розумних щоденних практик щодо здоров'я та безпеки вашої інформації в інтернеті» і серед іншого включає регулярне оновлення програмного забезпечення браузера, встановлення та підтримку програмного забезпечення для захисту, вибір надійних паролів, заборону ділитися паролями, а також уникнення загальнодоступного Wi-Fi для онлайн-банкінгу та інших фінансових операцій», що, зрештою, зменшить вірогідність контакту із кібершахраями та кіберзлодіями (Скибун, 2021, с. 42).

Кібергігієна – це передусім самооцінка своїх ризиків, тому важливо дотримуватись певних правил при користуванні гаджетами, і основними з них є такі: не підключатись до публічного Wi-Fi; не переходити за підозрілими посиланнями, які надсилають; не додавати незнайомих людей у друзі в соціальних мережах; змінювати паролі кожні 2–3 місяці, використовуючи різні складні комбінації, які важко вирахувати, та двофакторну аутентифікацію не через смс, а через додаток; встановлювати автоматичні оновлення версій програмного забезпечення; хоча б раз на кілька років відвідувати тренінги з кібербезпеки (Аушев, 2020).

Законом України «Про основні засади забезпечення кібербезпеки України», прийнятим 07 жовтня 2017 р., кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі ("Про основні засади", 2017). Тобто поняття кібербезпеки тлумачиться насамперед як убезпечення інформаційного простору держави і громадянина від можливих віртуальних загроз. Водночас наукове співтовариство має власні погляди на те, як саме тлумачити поняття кібербезпеки. Б. Кормич зазначає, що кібербезпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави. В. Остроухов пропонує наступне авторське визначення кібербезпеки – це стан захищеності особи, держави і суспільства, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди (Лісовська, 2019, с. 8–9). Таким чином, можна констатувати, що, попри наявне офіційне тлумачення поняття «кібербезпека», сьогодні існує чимало варіацій змістового наповнення і визначення цього терміна.

Натомість аналіз доступної літератури показав, що науковці сходяться на єдиному тлумаченні поняття «кіберзахист», закріпленому Законом України «Про основні засади забезпечення кібербезпеки України», який пояснює його як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів

криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем ("Про основні засади", 2017). У жовтні 2021 р. адміністрацією Держспецзв'язку було розроблено Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури ("Про затвердження Методичних рекомендаці", 2021), де визначено мету, складові рекомендацій, прописано систему заходів кіберзахисту, яка складається з чотирьох елементів: клас заходів кіберзахисту (організовує заходи кіберзахисту на системному рівні та визначає зміст циклу управління кібербезпекою); категорія заходів кіберзахисту (складові елементи класу заходів кіберзахисту, упорядковані за групою цільових результатів забезпечення кібербезпеки та тісно пов'язані із завданнями забезпечення кібербезпеки та конкретними групами заходів кіберзахисту); підкатегорія заходів кіберзахисту (складовий елемент категорії заходів кіберзахисту; містить сукупність конкретних заходів кіберзахисту, які сформульовані у вигляді конкретного результату, що має бути досягнутий під час упровадження заходів кіберзахисту); інформаційні посилання (елемент системи заходів кіберзахисту, який містить посилання на стандарти, нормативні документи, рекомендації та загальноприйняті практики, поширені у галузях (секторах) критичної інфраструктури для забезпечення безпеки) ("Про затвердження Методичних рекомендацій", 2021). Також варто наголосити, що Україна активно залучає американський та європейський досвід, міжнародні стандарти у сфері кіберзахисту. Фахівці із Держспецзв'язку, наприклад, розробили Загальні правила обміну інформацією про кіберінциденти (Протокол TLP) ("Загальні правила обміну", 2021), що відповідають рекомендації Європейської агенції з кібербезпеки (ENISA Considerations on the Traffic Light Protocol) та документу Форуму команд реагування та безпеки (FIRST Standards Definitions and Usage Guidance – версії 1.0 «Traffic Light Protocol»). Загальні правила визначають спосіб маркування повідомлень про кіберінциденти з метою обмеження кола осіб-сторін інформаційного обміну, які можуть мати доступ до повідомлення. Їх розроблено для сприяння правильному поширенню інформації.

Прийняття цього та подібних документів є надзвичайно актуальним, адже, згідно з дослідженнями, відсоток комп'ютерів, заражених шкідливими програмами, в Україні один із найвищих у світі і становить 28,7 %, тобто кожний третій комп'ютер інфікований шкідливими програмами. За таких умов вкрай важливим є обов'язкове використання комплексу програмних і апаратних засобів, які б дозволили забезпечити прийнятний рівень захищеності інфраструктури, а саме: ефективне надійне антивірусне програмне забезпечення, системи запобігання вторгнень, міжмережеві екрани, модулі контролю пристроїв і доступу до інтернету, системи шифрування даних, керування роботою мобільних пристроїв, засоби для захисту поштових серверів і систем колективної роботи тощо. Регулярне тестування на проникнення і перевірка конфігурацій дозволять виявити помилки до того, як хакери віднайдуть доступ до управління сервером або комп'ютером користувача (Трофименко та ін., 2019, с. 155).

Мінцифри та Держспецзв'язку продовжують ініціювати реформування у законодавстві, яке стосується кібербезпеки. Крім цього, нарощуються потужності

Державного центру кіберзахисту та працює урядова команда реагування на кіберінциденти CERT-UA. В Україні також діє один із найпотужніших у Європі кіберполігонів, що дозволяє відпрацьовувати сценарії реагування на кіберінциденти у режимі реального часу ("Україна посіла 25 місце", 2020). Позитивним кроком стало затвердження Указом Президента України № 447 від 26 серпня 2021 р. нової Стратегії кібербезпеки України на період до 2025 р. ("Про рішення Ради", 2021). У документі зазначається, що кіберпростір разом з іншими фізичними просторами визнано одним із можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить забезпечення захисту критичної інформаційної інфраструктури від кібератак, проведення превентивних наступальних операцій у кіберпросторі тощо. Останнім часом спостерігається використання кіберпростору терористичними організаціями – кібертерористами, мішенями яких залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо. Все це вимагає від українських спеціалістів вдосконалення системи кібернетичного захисту, реорганізації та оновлення стратегії боротьби із кіберзлочинцями. Крім того, нова стратегія пріоритетами при забезпеченні кібербезпеки визначає убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейську і євроатлантичну інтеграцію у сфері кібербезпеки ("Про рішення Ради", 2021). Стратегія передбачає також утворення у системі Міністерства оборони України кібервійськ і забезпечення їх належними фінансовими, кадровими та технічними ресурсами; запровадження у системах військово-патріотичного виховання та територіальної оборони навчальних програм підготовки і проведення практичних навчань у сфері кібербезпеки; завершення імплементації в законодавство України положень Конвенції про кіберзлочинність; врегулювання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі та ін.

На думку О. Трофименко, з метою посилення стійкості критичної національної інфраструктури з кібербезпеки український уряд регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на кіберінциденти. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС і НАТО посилюють спроможності нашої держави у сфері кібербезпеки і відповідають національним інтересам (Трофименко та ін., 2019, с. 153).

Важливим кроком вперед стало започаткування українськими закладами вищої освіти спеціальності 125 «Кібербезпека» (далі – «Кібербезпека»), що розвивається швидкими темпами та у кожному конкретному закладі має певну змістову градацію. Аналіз відкритих даних вступних кампаній закладів вищої освіти міста Києва за 2018–2022 роки у Єдиній державній електронній базі з питань освіти ("Вступна кампанія 2022", б.р.) продемонстрував, що з 2018 року кількість університетів, які пропонували вступ на спеціальність «Кібербезпека», упродовж остан-

ніх п'яти років зросла (рис. 1). До уваги бралися дані за небюджетними та відкритими конкурсними пропозиціями для вступу на денну і заочну форму навчання освітнього ступеня «бакалавр».

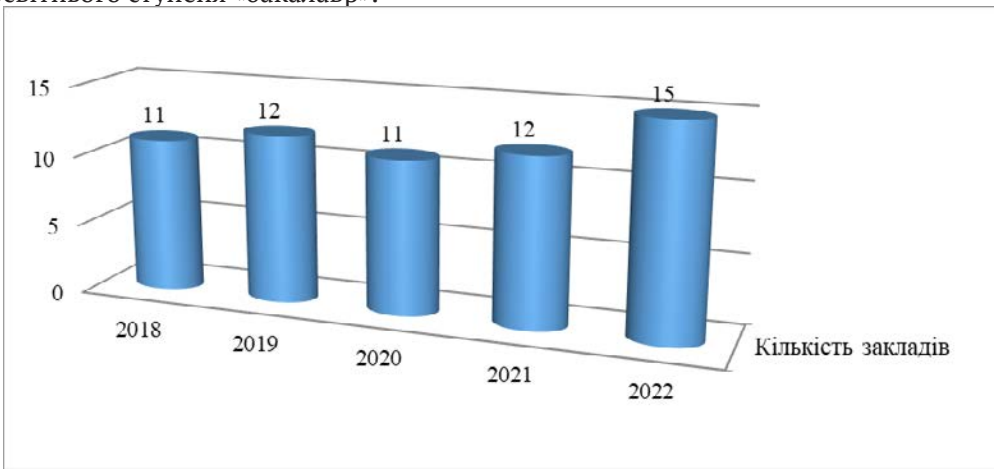

Рис. 1. Кількість закладів вищої освіти (м. Київ) із пропозиціями спеціальності «Кібербезпека»

Із 2021 року деякі заклади вищої освіти відкрили набір студентів на кілька окремих освітніх програм, які до цього часу були складовою частиною спеціальності «Кібербезпека». Станом на вересень 2022 року абітурієнти могли обрати освітню програму з такою ж назвою, як і спеціальність («Кібербезпека»), або обрати для себе більш вузький напрям підготовки (табл. 1).

Таблиця 1

Освітні програми спеціальності «Кібербезпека»
закладів вищої освіти (м. Київ)

Назва освітньої програми	Заклад вищої освіти
Кібербезпека	Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана» Заклад вищої освіти «Відкритий міжнародний університет розвитку людини «Україна» Київський національний університет імені Тараса Шевченка Маріупольський державний університет Національний університет біоресурсів і природокористування України Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна академія управління персоналом»» Приватний вищий навчальний заклад «Європейський університет»

Продовження табл. 1

Безпека інформаційних і комунікаційних систем; Безпека інформаційних і комунікаційних систем в економіці	Національний авіаційний університет Київський національний торговельно-економічний університет Київський національний університет будівництва і архітектури Київський університет імені Бориса Грінченка
Управління інформаційною безпекою; Управління інформаційною та кібернетичною безпекою	Державний університет телекомунікацій Національний авіаційний університет
Інформаційна та кібернетична безпека; Технічні системи інформаційного та кібернетичного захисту	Державний університет телекомунікацій
Системи технічного захисту інформації, автоматизація її обробки; Системи та технології кібербезпеки	Національний авіаційний університет
Інженерія кібербезпеки	Київський національний університет технологій та дизайну
Системи технічного захисту інформації; Системи, технології та математичні методи кібербезпеки	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Управління системами захисту інформації та кібернетичної безпеки	Київський університет інтелектуальної власності та права національного університету «Одеська юридична академія»

Порівнюючи кількість заяв, поданих у 2018–2022 роках до закладів вищої освіти м. Києва для вступу на денну і заочну форму навчання освітнього ступеня «бакалавр», також спостерігалася тенденція зростання. Так, у 2021 році, порівняно із 2020 роком, у всіх закладах вищої освіти кількість заяв зросла майже вдвічі. Таке ж збільшення попиту очікувалося у 2022 році, про що свідчить збільшення кількості як університетів, так і конкурсних пропозицій на спеціальність «Кібербезпека» (рис. 2).

Однак воєнна агресія росії проти України, розпочата 24 лютого 2022 року, істотно вплинула на очікування університетів щодо збільшення кількості абітурієнтів, охочих здобути освіту за спеціальністю «Кібербезпека». У зв'язку з масовим виїздом українців за кордон, серед яких і школярі випускних класів, показники вступної кампанії у 2022 році опинилися на рівні 2018–2020 років, коли спеціальність лише набувала популярності в Україні, а подекуди стали ще нижчими (табл. 2).

Попри невтішні кількісні показники цьогорічної вступної кампанії, що спричинені війною, широкий вибір освітніх програм у межах спеціальності «Кібербезпека» свідчить про те, що українські заклади вищої освіти не стоять осторонь змін та інновацій і активно реагують на виклики сьогодення. Відкриття та подальший розвиток окремих кафедр, що готують фахівців із кіберзахисту, кібербезпеки, відбуваються на високому професійному рівні, підтвердженням чого може слугувати факт, що українські випускники працюють у відомих світових ІТ-компаніях і будують там перспективну кар'єру.

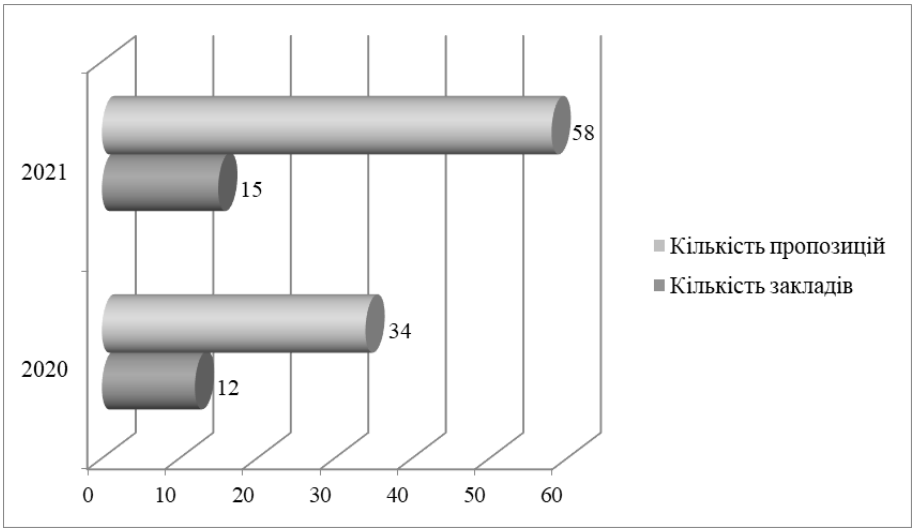

Рис. 2. Конкурсні пропозиції закладів вищої освіти (м. Київ) у 2020–2021 роках

Таблиця 2

Показники вступної кампанії за спеціальністю «Кібербезпека» (за даними закладів вищої освіти м. Києва) у 2018–2022 роках

Назва університету	Кількість поданих заяв				
	2018	2019	2020	2021	2022
Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана»	417	453	529	1083	521
Державний університет телекомунікацій	762	912	904	1706	934
Київський національний торговельно-економічний університет	288	468	794	1108	502
Київський національний університет будівництва і архітектури	259	253	338	638	289
Київський національний університет імені Тараса Шевченка	703	856	751	1376	820
Київський університет імені Бориса Грінченка	245	347	399	689	361
Маріупольський державний університет	83	88	100	134	33
Національний авіаційний університет	1665	1370	1529	3885	2133
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»	1655	1787	1864	2856	1638
Національний університет біоресурсів і природокористування України	–	278	343	604	338
Приватний вищий навчальний заклад «Європейський університет»	49	42	113	290	227

ВИСНОВКИ

Детально розглянувши питання забезпечення в Україні кіберзахисту інформації, кібербезпеки при користуванні мережею інтернет, кібергігієни, можемо сказати, що українські фахівці зробили значний крок уперед у цих питаннях, що засвідчують міжнародні статистичні дані. Поступово українське законодавство з питань кібербезпеки переорієнтовується на світові тенденції та запозичує позитивний іноземний досвід. Однак існують і невирішені досі нагальні питання, і одне з ключових – це зведення понятійного апарату кібербезпеки до закріплених на законодавчому рівні тлумачень. Важливим є також питання подальшого поглиблення міжнародного співробітництва у питаннях кіберзахисту та кібербезпеки, створення спільних міждержавних платформ для обміну інформацією. Варто, на нашу думку, залучати до державних програм із розробки стратегій, рекомендацій кібернетичної безпеки також і спеціалістів із приватних організацій або фірм, адже такий крок консолідує суспільство та сприятиме виробленню максимально ефективного продукту. Необхідно зробити загальнодоступною, поширювати у соціальних мережах та на офіційних сайтах інформацію щодо дотримання кібергігієни, правил та рекомендацій, яким чином цього досягати і для чого це потрібно. Ефективне розповсюдження подібної інформації забезпечить зниження ризиків при перебуванні людини у кіберпросторі.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

Аушев Є. Безпека в інтернеті: найпростіші правила захисту даних. *BBC News Україна* : офіц. вебсайт. 11 лют. 2020. URL: https://www.bbc.com/ukrainian/blogs-51444737 (дата звернення 28.08.2022).

Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* № 9. 2019. С. 100–107. DOI: https://doi.org/10.32849/2663-5313/2019.9.17

Вступна кампанія 2022. *Єдина державна електронна база з питань освіти*. URL: https://vstup.edbo.gov.ua/offers/ (дата звернення: 30.09.2022).

Головка А. Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни. *Молодий вчений.* 2016. № 4 (31). С. 333–336.

Деякі питання оптимізації системи центральних органів виконавчої влади : Постанова Кабінету Міністрів України від 2 верес. 2019 р. № 829. *Урядовий портал*. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-optimizaciyi-sistem-829 (дата звернення: 23.08.2022).

Загальні правила обміну інформацією про кіберінциденти. Протокол TLP. *Державна служба спеціального зв'язку та захисту інформації України* : офіц. вебсайт. 26.10.2021. URL: https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberincidenti-protokol-tlp (дата звернення: 23.08.2022).

Кібергігієна… Що це? І 5 речей, які слід знати про це. *Itech.* 18.03.2021. URL: https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ (дата звернення: 23.08.2022).

Кочан І. Слова з компонентом кібер- у сучасній українській мові. *Вісник Львівського університету. Серія філологічна.* 2016. Вип. 63. С. 277–285.

Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18 верес. 2019 р. № 856. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (дата звернення: 23.08.2022).

Про CERT-UA. *CERT-UA* : офіц. вебсайт. URL: https://cert.gov.ua/about-us (дата звернення: 23.08.2022).

Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 23.08.2022).

Про додержання прав людини під час проведення оперативно-технічних заходів : Указ Президента України від 7 листоп. 2005 р. № 1556/2005. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1556/2005#Text (дата звернення: 23.08.2022).

Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури : Наказ Адмін. Держспецзв'язку від 6 жовт. 2021 р. № 601. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=48543 (дата звернення: 23.08.2022).

Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.08.2022).

Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 23.08.2022).

Скибун О. Ж. Кібергігієна як складова формування цифрової держави. *Вісник Національної академії державного управління при Президентові України. Серія «Державне управління».* 2021. № 2 (101). С. 39–46.

Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150–157. DOI: https://doi.org/10.18372/2410-7840.21.13951

Україна посіла 25 місце у міжнародному рейтингу з кібербезпеки. *Урядовий портал* : офіц. вебсайт. 10 груд. 2020. URL: https://www.kmu.gov.ua/news/ukrayina-posila-25-misce-u-mizhnarodnomu-rejtingu-z-kiberbezpeki (дата звернення: 23.08.2022).

REFERENCES

Aushev, Ye. (2020, February 11). *Bezpeka v interneti: naiprostishi pravyla zakhystu danykh [Security on the Internet: the simplest rules of data protection]*. BBC News Ukraina. https://www.bbc.com/ukrainian/blogs-51444737 [in Ukrainian].

Bakalinska, O., & Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal provision of cyber security in Ukraine]. *Entrepreneurship, Economy and Law*, *9*, 100–107. https://doi.org/10.32849/2663-5313/2019.9.17 [in Ukrainian].

Vstupna kampaniia 2022 [Admission campaign 2022]. (n.d.). Yedyna derzhavna elektronna baza z pytan osvity. Retrieved September 30, 2022 from https://vstup.edbo.gov.ua/offers/ [in Ukrainian].

Holovka, A. (2016). Zakhyst kiberprostoru yak skladova informatsiinoi bezpeky Ukrainy v umovakh hibrydnoi viiny [Cyberspace protection as a component of Ukraine's information security in conditions of hybrid warfare]. *Young Scientist*, *4*(31) 333–336 [in Ukrainian].

Cabinet of Ministers of Ukraine. (2019, September 2). *Deiaki pytannia optymizatsii systemy tsentralnykh orhaniv vykonavchoi vlady [Some issues of optimization of the system of central executive bodies]* (Resolution No. 829). Government portal. https://www.kmu.gov.ua/npas/deyaki-pitannya-optimizaciyi-sistem-829 [in Ukrainian].

State Service of Special Communications and Information Protection of Ukraine. (2021, October 26). *Zahalni pravyla obminu informatsiieiu pro kiberintsydenty. Protokol TLP [General rules for exchanging information about cyber incidents. TLP protocol]*. Retrieved August 23, 2022 from https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberincidenti-protokol-tlp [in Ukrainian].

Kiberhihiiena… Shcho tse? I 5 rechei, yaki slid znaty pro tse [Cyber hygiene… What is it? And 5 things to know about it]. (2021, March 18). Itech. https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ [in Ukrainian].

Kochan, I. (2016). Slova z komponentom kiber- u suchasnii ukrainskii movi [The words with component cyber- in modern ukrainian language]. *Visnyk of the Lviv University. Series Philology*, *63*, 277–285 [in Ukrainian].

Lisovska, Yu. (2019). *Kiberbezpeka: ryzyky ta zakhody [Cyber security: risks and measures]*. Kondor [in Ukrainian].

Cabinet of Ministers of Ukraine. (2019, September 18). *Pytannia Ministerstva tsyfrovoi transformatsii [Issues of the Ministry of Digital Transformation]* (Resolution No. 856). https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text [in Ukrainian].

Pro CERT-UA [About CERT-UA]. (n.d.). CERT-UA. Retrieved August 23, 2022 from https://cert.gov.ua/about-us [in Ukrainian].

Verkhovna Rada of Ukraine. (2006, February 23). *Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy [On the State Service for Special Communications and Information Protection of Ukraine]* (Law No. 3475-IV). https://zakon.rada.gov.ua/laws/show/3475-15#Text [in Ukrainian].

President of Ukraine. (2005, November 7). *Pro doderzhannia prav liudyny pid chas provedennia operatyvno-tekhnichnykh zakhodiv [On the observance of human rights during operational and technical measures]* (Decree No. 1556/2005). https://zakon.rada.gov.ua/laws/show/1556/2005#Text [in Ukrainian].

State Service of Special Communications and Information Protection of Ukraine. (2021, October 6). *Pro zatverdzhennia Metodychnykh rekomendatsii shchodo pidvyshchennia rivnia kiberzakhystu krytychnoi informatsiinoi infrastruktury [On the approval of Methodological recommendations for increasing the level of cyber protection of critical information infrastructure]* (Order No. 601). https://cip.gov.ua/services/cm/api/attachment/download?id=48543 [in Ukrainian].

Verkhovna Rada of Ukraine. (2017, October 5). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Cybersecurity in Ukraine]* (Law No. 2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

President of Ukraine. (2021, August 26). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]* (Decree No. 447/2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

Skybun, O. Zh. (2021). Kiberhihiiena yak skladova formuvannia tsyfrovoi derzhavy [Cybergigiena as a component of the formation of a digital state]. *Bulletin of the National Academy of Public Administration under the President of Ukraine. Series "Public Administration"*, *2*(101), 39–46 [in Ukrainian].

Trofymenko, O., Prokop, Yu., Lohinova, N., & Zadereiko, O. (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu [Cybersecurity of Ukraine: Analysis of the current situation]. *Ukrainian Information Security Research Journal*, *21*(3), 150–157. https://doi.org/10.18372/2410-7840.21.13951 [in Ukrainian].

Ukraina posila 25 mistse u mizhnarodnomu reitynhu z kiberbezpeky [Ukraine ranked 25th in the National Cyber Security Index]. (2020, December 10). Government portal. https://www.kmu.gov.ua/news/ukrayina-posila-25-misce-u-mizhnarodnomu-rejtingu-z-kiberbezpeki [in Ukrainian].

UDC 004.946.5.056:316.3(477)

Zoriana Sverdlyk,
PhD in Historical Sciences, Associate Professor,
Associate Professor of Informational
Technologies Department,
Kyiv National University of Culture and Arts
(Kyiv, Ukraine)
e-mail: zsverdlyk@gmail.com
ORCID: 0000-0002-2104-0920

CYBER SECURITY AND CYBER PROTECTION: TOPICS ON THE AGENDA IN UKRAINIAN SOCIETY

The aim of the article is to analyse the concepts of «cyber hygiene», «cyber security», «cyber protection», and clarify the role of those processes which are interpreted by these terms in modern human life; to identify the main achievements in Ukrainian law system regarding the legal cybernetic sphere regulation; to highlight key rules for observing cyber hygiene.

The research methodology has been implemented using scientific methods of terminological analysis when comparing the definitions of relevant terms. Statistical method has been used in order to generalise quantitative indicators characterising the increase in the interest of higher education establishments in cyber security specialists training. Comparison and generalisation have made it possible to comprehensively reveal the raised problem in this study.

The scientific novelty of this research consists in the following: emphasising the cooperation importance and necessity of Ukrainian organisations with foreign partners in the sphere of information protection contained in cyber space; identifying and tracking tendencies in improving cyber security in the context of science, education and state administration.

Conclusions. The issue studying of ensuring information cyber protection, as well as cyber security when using Internet and cyber hygiene in Ukraine, has highlighted the vision that Ukrainian specialists have made a significant step forward in these matters. This is confirmed by international statistical data.

The analysis of recently adopted legislative, normative legal acts and regulatory documents at the national level has confirmed the thesis that Ukrainian legislation in cyber security issues is gradually reorienting itself to global tendencies, and borrowing positive foreign experience. However, there still exist urgent unresolved problems, the basis of which is the reduction of the conceptual cyber security apparatus to fixed at the legislative level interpretations.

The issues of further international cooperation intensification in matters of cyber protection and cyber security, additionally, creation of common interstate platforms for information exchange, are necessary as well.

No less important is the development and expansion of educational programmes in speciality 125 «Cyber Security» in higher education establishments of Ukraine. According to the obtained results of this study, the interest in this profession among youth has been growing recently.

Keywords: cyber hygiene, cyber protection, cyber security, Internet network, speciality "Cyber security", cyber threat, law, recommendation.

Стаття надійшла до редакції 30.09.2022 р.