УДК 338.439
DOI https://doi.org/10.24144/2307-3322.2025.88.4.35

ОСОБЛИВОСТІ ВИКЛАДАННЯ ІНФОРМАЦІЙНИХ ДИСЦИПЛІН: ВРАХУВАННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСИТЕМ ТА КОМПЛЕКСІВ

Бундз Р.О.,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного та кримінального права
Навчально-наукового інституту права,
психології та інноваційної освіти
Національного університету «Львівська політехніка»
ORCID: 0000-0002-3651-4068
e-mail: rostyslav.o.bundz@lpnu.ua

Ших Д.М.,
ФОП
ORCID: 0009-0005-2772-1830
e-mail: danyil.shykh@gmail.com

Бундз Р.О., Ших Д.М. Особливості викладання інформаційних дисциплін: врахування безпеки інформаційних систем та комплексів.

У сучасну епоху формування інформаційного суспільства роль інформаційної безпеки та кібербезпеки стрімко зростає, що обумовлює необхідність формування ефективної державної політики та підготовки кваліфікованих кадрів у цій сфері. У статті проаналізовано еволюцію підходів до захисту національних інтересів України в інформаційній сфері та акцентовано увагу на важливості інформаційної та кібербезпеки як інтегральних і самостійних складових національної безпеки. Підкреслюється, що сучасні загрози набувають нових форм, а традиційні методи ведення війни доповнюються інформаційним і кібернетичним протиборством.

У статті особливу увагу приділено освітнім аспектам підготовки фахівців з інформаційної безпеки. Окреслено основні педагогічні підходи до викладання дисциплін із кібербезпеки, такі як традиційний лекційний формат, підхід скрайбів, запрошення експертів, самостійне навчання, проєктне навчання, синергія досліджень та навчання, а також методика атака/захист у лабораторних умовах. Розглядаються переваги і недоліки кожного з підходів, акцентується на важливості розвитку критичного мислення, творчості й аналітичних навичок у студентів.

Проаналізовано також результати міжнародних освітніх і науково-дослідних проєктів за участю студентів, зокрема CRDF Global і TEMPUS ENGENSEC. Наведено приклади реалізації STEM-підходу в навчанні кібербезпеці через участь студентів у розробці методів автентифікації пристроїв за допомогою фізичних характеристик електронних компонентів, а також через ігрові освітні проєкти з формування навичок кібергігієни серед студентів нефахових спеціальностей.

У роботі підкреслюється важливість мотивації студентів до вивчення кібербезпеки, зокрема через використання таких моделей, як тріархічна теорія інтелекту Стенберга і таксономія Блума, що сприяють комплексному розвитку аналітичних, практичних і творчих навичок. Окрему увагу приділено впровадженню методу eduScrum для підвищення когнітивної активності студентів у процесі навчання і розробки освітніх і дослідницьких проєктів.

Результати дослідження доводять, що інтеграція активних методик навчання та залучення студентів до практичної діяльності у сфері кібербезпеки є ключовими чинниками формування висококваліфікованих фахівців, здатних ефективно захищати національні інтереси в умовах інформаційної війни та глобальних кіберзагроз. Отримані висновки можуть бути використані для подальшого вдосконалення освітніх програм, підготовки кадрів для сектору безпеки і оборони України, а також для розробки національних стратегій розвитку інформаційної безпеки.

Ключові слова: кібербезпека, безпека, національна безпека, інформаційна безпека, кіберзагроза, STEM, метод Scrum, таксономія Блума, навички комунікації, CRDF Global.

Bundz R.O., Shukh D.M. Features of teaching information disciplines: taking into account the security of information systems and complexes.

In today's era of information society formation, the role of information security and cybersecurity is rapidly increasing, which necessitates the formation of an effective state policy and training of qualified personnel in this area. The article analyses the evolution of approaches to protecting Ukraine's national interests in the information sphere, examines the content of the basic concepts and focuses on the importance of information and cybersecurity as integral and independent components of national security. It is emphasised that modern threats are taking on new forms, and traditional methods of warfare are being supplemented by information and cyber confrontation.

The article pays special attention to the educational aspects of training information security specialists. The author outlines the main pedagogical approaches to teaching cybersecurity disciplines, such as the traditional lecture format, the scrub approach, inviting experts, self-study, project-based learning, research and teaching synergy, and the attack/defence methodology in the laboratory. The advantages and disadvantages of each approach are discussed, with an emphasis on the importance of developing students' critical thinking, creativity and analytical skills.

The results of international educational and research projects involving students, such as CRDF Global and TEMPUS ENGENSEC, are also analysed. Examples of the implementation of the STEM approach to cybersecurity education through student participation in the development of device authentication methods using the physical characteristics of electronic components, as well as through game-based educational projects to develop cyber hygiene skills among students of non-field-specific specialties are presented.

The paper emphasises the importance of motivating students to study cybersecurity, in particular through the use of models such as Stenberg's triarchic theory of intelligence and Bloom's taxonomy, which promote the integrated development of analytical, practical and creative skills. Particular attention is paid to the implementation of the eduScrum method to increase students' cognitive activity in the learning process and the development of educational and research projects.

The results of the study prove that the integration of active teaching methods and the involvement of students in practical cybersecurity activities are key factors in the formation of highly qualified specialists capable of effectively protecting national interests in the context of information warfare and global cyber threats. The findings can be used to further improve educational programmes, train personnel for the security and defence sector of Ukraine, and develop national strategies for the development of information security.

Key words: cybersecurity, security, national security, information security, cyber threat, STEM, Scrum method, Bloom's taxonomy, communication skills, CRDF Global.

Постановка проблеми. У сучасних умовах глобальної інформатизації суспільства інформаційна безпека та кібербезпека стали одними з ключових аспектів забезпечення національної безпеки. Зростаюча залежність держав, бізнесу і громадян від інформаційних систем обумовлює появу нових викликів і загроз. Постійне вдосконалення методів кібератак, гібридних загроз та інформаційно-психологічного впливу вимагає не лише технічного захисту інформаційного простору, а й комплексної підготовки висококваліфікованих фахівців. Проблема ускладнюється браком практично орієнтованої підготовки студентів та недостатньою інтеграцією теоретичних знань із практичними навичками в освітніх програмах.

Мета дослідження – проаналізувати сучасні виклики у сфері підготовки спеціалістів з інформаційної безпеки та кібербезпеки, узагальнити основні підходи до навчання інформаційної безпеки, зокрема традиційні лекційні методи, практико-орієнтовані проєктні підходи, методи атаки/захисту в ізольованих середовищах та впровадження гнучких методологій управління навчальним процесом (Scrum, eduScrum).

Стан опрацювання проблематики. Проблемі підготовки фахівців з інформаційної безпеки активно приділяли увагу такі науковці, як: Мет Бішоп, Дебора Фрінк, Лінет Древін, Авіель Девід Рубін, Маріліо Кардосо та багато інших.

Виклад основного матеріалу. У сучасну епоху формування інформаційного суспільства – суспільства, в якому більшість працездатного населення задіяна в інформаційній сфері – спостері-

гається активний розвиток новітніх форм досягнення політичних, економічних та інших цілей на інформаційному рівні. Саме тому в системах національної безпеки розвинених держав передбачено розробку і реалізацію комплексних національних стратегій, що включають політичні, воєнні, економічні, соціальні та інформаційні напрями. Особливе значення надається саме інформаційним стратегіям, які забезпечують ефективне функціонування інших стратегічних напрямків.

В останні десятиліття роль інформаційної безпеки стрімко зростає. Інформаційний потенціал стає визначальним чинником у процесі прийняття державних рішень, створенні сучасних озброєнь, організації пропагандистської діяльності, а також у підтримці боєздатності власних та союзницьких сил.

Традиційна концепція «тотальної війни» поступово втрачає актуальність. На зміну їй приходять нові форми протиборства – так звані «цивілізовані» війни, де досягнення політичних та економічних цілей здійснюється шляхом інформаційного впливу, а не прямого військового вторгнення.

В інформаційну епоху «нетрадиційні» загрози, зокрема інформаційні війни, набули визначальної ваги як один із найбільш ефективних інструментів реалізації національних інтересів провідними державами світу.

Україна, враховуючи своє геополітичне положення та інтереси розвинених і сусідніх держав, постійно зазнає інформаційно-психологічного впливу, що обумовлює високу ймовірність її втягнення в інформаційне протистояння.

Проблеми забезпечення інформаційної безпеки сьогодні набувають особливого значення. Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки стоїть в одному ряду із захистом суверенітету, територіальної цілісності та економічної стабільності держави [1].

Державна політика у сфері інформаційної безпеки є невід'ємною складовою національної безпеки та передбачає створення системи поглядів і заходів, спрямованих на розвиток і захист інформаційної сфери, мінімізацію негативного впливу зовнішніх інформаційних загроз.

Інформаційна безпека є одночасно самостійною сферою національної безпеки та її важливою складовою. Інформаційні ресурси, технології та інфраструктура відіграють вирішальну роль у соціально-економічному, науково-технічному та культурному розвитку країни.

Особливої уваги набуває питання кібербезпеки. Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента 26 серпня 2021 року, забезпечення кібербезпеки визнано пріоритетним напрямком державної політики. Стратегія визначає кіберпростір як повноцінний театр воєнних дій, де поряд із захистом критичної інфраструктури здійснюються превентивні наступальні кібероперації [2].

Серед основних загроз кібербезпеці України і світу залишається агресивна політика Російської Федерації, що поєднує кібератаки та інформаційно-психологічні операції в межах гібридної війни.

Розвиток ЗМІ, інформаційних технологій та цифрової інфраструктури зробив інформаційне протиборство масштабнішим і результативнішим. Сучасне протиборство часто переноситься в кіберпростір, де інформація стає потужним інструментом політичного та економічного впливу.

Таким чином, на сьогодні геополітична вага держави визначається не тільки економічною чи військовою могутністю, а й здатністю ефективно діяти в інформаційній сфері: впливати на інтелектуальний потенціал інших країн, формувати світоглядні орієнтири та підривати ідеологічні основи суперників.

Інформаційне суспільство, глобальний інформаційний простір і кіберпростір стали невід'ємною частиною світового розвитку. Однак із ними з'явилися і нові загрози: кіберзлочинність, кібертероризм, інформаційні війни.

Для ефективної протидії новим викликам необхідні висококваліфіковані фахівці у сфері кібербезпеки, здатні забезпечити захист інформаційних ресурсів і національних інтересів України.

Саме тому формування кадрового потенціалу в сфері інформаційної безпеки та кібербезпеки – один із ключових напрямів державної політики. Здобувачі вищої освіти отримують знання та навички, необхідні для роботи в Службі безпеки України, Міністерстві оборони України, Державній службі спеціального зв'язку та інших структурах.

Посібники, орієнтовані на підготовку таких спеціалістів, стають важливим освітнім ресурсом, сприяючи реалізації державних програм та підвищенню рівня кіберзахисту держави.

У навчанні кібербезпеці важливо орієнтуватися на Тріархічну теорію інтелекту Стенберга та таксономію Блума. Використання тріархічної моделі допомагає формувати аналітичні, практичні

та креативні навички студентів через командну роботу, тоді як таксономія Блума допомагає структурувати навчальні цілі залежно від рівня складності мислення й розв'язання проблем [3, 4].

Ці методи навчання були успішно реалізовані в міжнародних проєктах за участю студентів технічних і нетехнічних спеціальностей. Зокрема, результати досліджень, описані у статті, були отримані під час роботи над проєктами організації CRDF Global – незалежної неприбуткової організації, що підтримує міжнародну науково-технічну співпрацю через гранти, ресурси, освіту і сервіси.

Одним із таких науково-дослідних проєктів було підвищення захисту пристроїв для обробки інформації (комп'ютерів, планшетів, мобільних телефонів) шляхом використання методів автентифікації, заснованих на фізичних відмінностях пристроїв, що виникають ще під час виробництва. Відмінності у внутрішньому електричному шумі дозволяють надійно ідентифікувати пристрої без використання додаткових зовнішніх засобів, що значно підвищує точність автентифікації.

У попередніх дослідженнях, де працювали викладачі та магістри, було розроблено метод автентифікації персональних комп'ютерів за електричними характеристиками. Робота в цьому науковому проєкті продемонструвала інтегрований підхід STEM у навчанні кібербезпеці: студентам потрібно було розуміти фізику сигналів у пристроях (наука), технології збору сигналів через аудіокарти (технології), розробку програмного забезпечення для передачі даних (інженерія) і математичну обробку даних для виділення ознак автентифікації (математика).

Ще одним проєктом, результати якого висвітлені в статті, став освітній проєкт із навчання основам кібергігієни. У ньому брали участь студенти, спеціальності яких не пов'язані з кібербезпекою, проте для яких навички кібергігієни є соціально важливими. Навчання проходило у форматі ігрових ситуацій: студенти досліджували наслідки своїх дій на ноутбуках, смартфонах та комп'ютерах, після чого проходили тестування [5].

З метою підвищення когнітивної активності студентів у цих проєктах застосовувався метод Scrum.

Бажання інтегрувати принципи управління проєктами Scrum у освіту призвело до появи методу eduScrum. З 2015 року eduScrum активно використовується у школах та університетах Нідерландів. Практика показує, що навчальні результати при застосуванні eduScrum зростають у середньому на 20% у порівнянні з класичними методами.

Головна ідея eduScrum полягає у делегуванні частини відповідальності за навчання самим студентам. Оскільки це agile-методологія, вона визначає, «що» і «чому» потрібно робити, але не жорстко регламентує, «як» це має бути реалізовано.

Методика eduScrum включає обов'язкові структурні елементи: ролі, події, елементи та правила. Основна увага приділяється організації та своєчасному виконанню завдань. Успішні приклади використання eduScrum описані у викладанні інженерних дисциплін, навчанні програмуванню мікроконтролерів Arduino, створенні віртуальних лабораторій, інтерактивних курсах з JavaScript у системі Moodle та в інженерних курсах.

Освіта XXI століття має змінюватися відповідно до потреб швидкозмінного виробництва, і методики на кшталт eduScrum сприяють розвитку самостійності та відповідальності студентів, що дозволяє їм краще адаптуватися до реальної професійної діяльності. [6]

Участь студентів у проєктах CRDF Global надала їм можливість глибше дослідити проблематику кібербезпеки. Зокрема, вони ознайомилися з перспективними методами захисту, які ґрунтуються на використанні своєрідної «біометрії» пристроїв для створення складніших паролів, що значно ускладнює проведення кібератак.

Отримані результати вказують на можливість ідентифікації серійних комп'ютерів, які на перший погляд є абсолютно однаковими. Невеликі відмінності між пристроями допускаються на рівні компонентів через виробничі допуски й технологічні відхилення.

Висновки. Особливо важливим є розвиток практичних навичок аналізу ризиків, проєктування захищених інформаційних систем, ідентифікації кіберінцидентів та побудови стратегій відновлення після атак. Спрямованість навчального процесу на командну взаємодію сприяє формуванню вмінь, необхідних для роботи у мультидисциплінарних середовищах, що є реальністю сучасної кібербезпеки.

Участь студентів у розробці та реалізації практичних проєктів, орієнтованих на автентифікацію пристроїв за їх фізичними характеристиками, показала перспективність впровадження STEM-підходу в освітні програми з кібербезпеки. Такі дослідження формують у студентів комп-

лексне розуміння взаємозв'язку фізичних, технічних і математичних аспектів інформаційної безпеки.

Аналіз міжнародного досвіду доводить, що впровадження інноваційних методик навчання, таких як eduScrum, дозволяє не лише підвищити навчальні результати, а й формувати у студентів високу академічну мобільність, готовність до самостійного професійного розвитку та здатність швидко адаптуватися до змінних умов у сфері кібербезпеки.

Таким чином, майбутнє підготовки фахівців у сфері інформаційної безпеки має базуватися на:

- комплексному поєднанні теорії і практики;
- впровадженні активних форм навчання та гейміфікації освітнього процесу;
- розвитку дослідницьких навичок через участь у міжнародних проєктах;
- формуванні навичок командної роботи й управління проєктами;
- постійному оновленні освітніх програм відповідно до новітніх технологічних і безпекових викликів.

Тільки завдяки такому системному підходу Україна зможе забезпечити належний рівень захисту свого інформаційного простору, посилити позиції в міжнародній кіберспільноті та підготувати нове покоління висококваліфікованих фахівців, здатних ефективно відповідати на виклики глобального інформаційного суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4215 (дата звернення: 28.04.2025).
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 28.04.2025).
3. Hamman, S.T., Hopkinson, K.M. (2016) Teaching Adversarial Thinking for Cybersecurity. J. Colloq. Inf. Syst. Secur. Educ. (CISSE) 4, p. 1–19.
4. Anderson, L.W., Krathwohl, D.R. (2001) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete, ed.; Addison Wesley Longman, Inc.: New York, NY, USA.
5. CRDF Global. URL: https://www.crdfglobal.org.
6. What Is eduScrum. URL: https://www.betterday.nl/eduscrum.