КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.183204
УДК 001.89:004.056

Соколов Володимир Юрійович
к.т.н., доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Складанний Павло Миколайович
к.т.н., доцент
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТРАТЕГІЙ ПОБУДОВИ ДРУГОГО ТА ТРЕТЬОГО РІВНЯ ОСВІТНІХ ПРОГРАМ ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА»

Анотація. В статті проаналізований світовий ринок з надання освітніх послуг в сфері інформаційної безпеки та кібербезпеки. Дослідження має на меті порівняти стратегій побудови навчальних програм для другого та третього освітнього рівня для спеціальностей, пов'язаних з інформаційними технологіями, інформаційною та кібербезпекою, а також сформувати рекомендації для гармонізації процесу навчання та міжнародних стандартів. Програми підготовки спеціалістів з кібербезпеки надто швидко застарівають. Оновлення ISO-стандартів проходить приблизно кожні чотири роки. Також стандарт для спеціальності 125 «Кібербезпека» для третього освітнього рівня ще потребує доопрацювання. З'являється проблема формування послідовного процесу впровадження новітніх підходів і практик в навчальні програми. Зростання ринку інформаційних технологій призводить до розширення потреб в спеціалістів з кібербезпеки. Видно, що одночасно відбуваються два процеси: перехід від практичних навичок до фундаментальних знань і навпаки. Найуспішнішими є ті заклади вищої освіти, які можуть комбінувати обидва підходи одночасно. Але для цього потрібно мати в своєму складі експериментальну базу, практичні навчальні лабораторії та штат викладачів і науковців. Таку задачу можуть виконувати лише великі установи. Так як виклики в кібербезпеці постійно змінюються, то від закладів вищої освіти вимагається вдосконалювати свої програми щорічно. Одночасно з процесом оновлення підходів до викладання проходять процеси вдосконалення корпусі міжнародних та галузевих стандартів, а також різноманітних кращих практик та фреймворків. Швидка зміна вимагає не тільки від викладачів постійного вдосконалення, але і від практикуючих фахівців з кібербезпеки. Таким чином, процес постійного навчання має продовжуватися й після формального закінчення магістратури чи аспірантури. В результаті даного дослідження видно, що лише комплексне формування навичок з інформаційної безпеки дозволяє якісно підготувати фахівців. На базі цього приведені вимоги до освітнього стандарту для підготовки спеціалістів та науковців.

Ключові слова: кібербезпека; інформаційна безпека; ІБ; інформаційні технології; ІТ; захист інформації; вразливості; навчальний процес; освітній стандарт.

ВСТУП

Інформаційна безпека (ІБ) або кібербезпека — це динамічна галузь, що швидко розвивається. Нові загрози, вразливості та технології з'являються часто, що вимагає від професіоналів постійної обізнаності з останніми розробками. Програми вищої освіти

можуть не встигати за цими змінами через час, необхідний для розробки та оновлення навчальних планів, а також через жорстку структуру академічних програм.

Постановка проблеми. Програми підготовки спеціалістів з кібербезпеки надто швидко застарівають. Оновлення ISO-стандартів проходить приблизно кожні чотири роки. Також стандарт для спеціальності 125 «Кібербезпека» для третього освітнього рівня ще потребує доопрацювання. З'являється проблема формування послідовного процесу впровадження новітніх підходів і практик в навчальні програми. Зростання ринку інформаційних технологій призводить до розширення потреб в спеціалістів з кібербезпеки.

Аналіз останніх досліджень і публікацій. В попередній роботі [1] були розглянуті підходи до формування наукового мислення у здобувачів вищої освіти з кібербезпеки. Але проблематика була розглянута лише зі сторони відповідності навчальних програм до потреб бізнесу. Такий підхід виправданий для здобувачів першого освітнього рівня, але не може застосовуватися для наукових рівнів освіти, бо вимоги бізнесу стосуються вирішення поточних проблем, а не діють на випередження.

Крім того, сучасному спеціалісту з ІБ для розвитку практичних навичок критично не вистачає практик по розрахунку, наприклад, ризиків [2] та SWOT-аналізу [3]. Звичайно стандарти не часто описують конкретні методики для розрахунку стійкості систем до зовнішніх втручань.

В роботах [4] і [5] представлені підходи до формування практичних навичок студентів з кібербезпеки та запропоновані моделі для тренування майбутніх спеціалістів.

Дослідження має на **меті** порівняти стратегій побудови навчальних програм для другого та третього освітнього рівня для спеціальностей, пов'язаних з інформаційними технологіями, інформаційною та кібербезпекою, а також сформувати рекомендації для гармонізації процесу навчання та міжнародних стандартів.

МЕТОДИКА ДОСЛІДЖЕННЯ

В даній статті використовується аналіз різних освітніх рівнів для спеціалістів з кібербезпеки. В якості об'єкту дослідження використовуються галузеві та міжнародні стандарти з ІБ. Основним методом дослідження є критичний аналіз підходів до впровадження наукових методів дослідження для здобувачів другого та третього освітнього.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд світового ринку надання освітніх послуг з інформаційної безпеки

Порівняння закладів вищої освіти Європи, Америки та Азії (див. табл. 1), які готують фахівців з ІБ, виявляє відмінні риси та сильні сторони в цих регіонах.

Таблиця 1

Співавторство зі здобувачами освіти за останні шість років

Аспект	Європейські університети	Американські університети	Азіатські університети
Напрямок розвитку спеціаліста	Сильний акцент на теорії та дослідженнях	Практична спрямованість та галузева приналежність	Поєднання теорії та практичних навичок

Міждисциплінарний підхід	Інтеграція різних галузей, таких як інформатика, математика та соціальні науки	Акцент на співпраці між комп'ютерними науками, інженерією та бізнес-дисциплінами	Інтегрують технології, інженерію та бізнес-дисципліни
Практичність	Фокус на основоположних принципах і теоретичних концепціях	Основний акцент на практичному навчанні та реальному застосуванні	Збільшення акценту на практичних навичках та навчанні на власному досвіді
Індустріальна співпраця	Співпраця з промисловістю, державними установами та науково-дослідними інститутами	Галузеві партнерства через стажування та дослідницьку співпрацю	Галузева співпраця
Галузева актуальність	Сильна увага до правил конфіденційності та захисту даних	Задоволення нагальних потреб галузі та вирішення нових викликів безпеці	Адаптація до регіональних потреб галузі та нових кіберзагроз
Можливості для досліджень	Акцент на теоретичних засадах та дослідженнях	Можливості для передових досліджень та інновацій	Зростаючі дослідницькі можливості та концентрація на інноваціях
Міжнародна перспектива	Залучання міжнародного студентства, пропонуючи мультикультурне навчальне середовище	Глобальна перспектива з різноманітним студентським складом та доступом до міжнародних галузевих практик	Зростаючий акцент на інтернаціоналізацію та глобальну співпрацю
Академічна структура	За Болонським процесом зі структурованими програмами навчання	Широкий спектр освітніх програм, включаючи спеціалізовані сертифікати та програми навчання для керівників	Слабко структуровані

Виходячи з результатів, представлений в табл. 1 можна виділити основні недоліки європейської системи освіти:

• *Обмежений практичний досвід*. Програми вищої освіти в галузі ІБ часто зосереджені на теоретичних знаннях і фундаментальних концепціях. Однак вони можуть мати обмежені можливості для отримання студентами практичного досвіду в реальних умовах. Ця практична прогалина іноді може призвести до того, що випускники не матимуть необхідних навичок та досвіду для негайного вирішення складних проблем безпеки у професійному середовищі.

• *Обмежена галузева співпраця*. Деякі заклади вищої освіти в ЄС можуть мати обмежену співпрацю з галузевими партнерами та організаціями. Це може призвести до розриву між академічною програмою та практичними потребами й очікуваннями роботодавців. Це також може призвести до застарілого або менш актуального змісту курсів, який не відповідає галузевим тенденціям і потребам.

• *Відсутність фокусу на спеціалізацію*. ІБ охоплює різні підгалузі, такі як мережева безпека, криптографія, реагування на інциденти та розробка безпечного програмного забезпечення. Програми вищої освіти часто надають широкий огляд цих тем, але можуть не пропонувати поглибленої спеціалізації в конкретних сферах. Студентам, які шукають спеціалізовані знання чи досвід, може знадобитися доповнити свою освіту додатковими сертифікатами, семінарами чи самостійним навчанням.

• *Обмежена практична складова*. Деякі програми вищої освіти можуть бути більш теоретично орієнтованими, зосереджуючись на дослідженнях та академічних заняттях, а

не на практичному застосуванні. Це може призвести до розриву між знаннями, отриманими під час навчання, та навичками, необхідними для виконання реальних ролей у сфері ІБ. Студентам, можливо, доведеться активно шукати можливості для практичного застосування та навчання поза межами формальної навчальної програми.

• *Вартість і доступність*. Вища освіта в ЄС може бути дорогою, особливо для іноземних студентів. Плата за навчання, витрати на проживання та інші супутні витрати можуть бути значними перешкодами для осіб, які прагнуть отримати освіту в галузі ІБ.

Основні виклики інформаційній безпеці

Не залежно від наповнення освітніх програм основні виклики при навчанні кібербезпеці зачіпають основні практичні питання:

1. Неадекватні політики паролів, такі як використання *слабких паролів* або повторне використання одного і того ж пароля в декількох облікових записах, можуть бути використані зловмисниками.

2. *Вразливості в програмному забезпеченні*, включаючи операційні системи, веб-браузери та сторонні програми, можуть бути використані зловмисниками для отримання несанкціонованого доступу або виконання шкідливого коду.

3. *Фішинг* полягає в тому, щоб змусити користувачів розкрити конфіденційну інформацію, таку як облікові дані для входу в систему або фінансові дані, за допомогою оманливих електронних листів, веб-сайтів або миттєвих повідомлень.

4. Методи *соціальної інженерії* використовують людську психологію для маніпулювання людьми, щоб змусити їх розкрити конфіденційну інформацію або виконати дії, які можуть поставити під загрозу безпеку.

5. Якщо не встановлені виправлення та *оновлення* для програмного забезпечення та систем, вони можуть стати вразливими до відомих експлойтів та атак.

6. Неправильно налаштовані параметри безпеки: Неправильно налаштовані параметри безпеки, такі як слабкий контроль доступу або неправильні конфігурації брандмауера, можуть призвести до несанкціонованого доступу або витоку конфіденційної інформації.

7. *SQL-ін'єкція* виникає, коли зловмисники використовують уразливості у веб-додатках для вставки шкідливого SQL-коду, що потенційно може призвести до несанкціонованого доступу або маніпуляцій з базовими базами даних.

8. *Міжсайтовий скриптинг* (XSS) дозволяєть зловмисникам впроваджувати шкідливі скрипти на веб-сторінки, які переглядають користувачі, що може призвести до компрометації їхніх облікових записів або викрадення конфіденційної інформації.

9. Недостатня перевірка валідації та авторизації може дозволити зловмисникам отримати *прямий доступ до чутливих об'єктів* у додатку або маніпулювати ними.

10. *Внутрішні загрози* пов'язані зі зловмисними або недбалими діями осіб з авторизованим доступом до систем або даних, що потенційно можуть призвести до несанкціонованого доступу, витоку даних або саботажу.

11. Вразливості *фізичної безпеки*, такі як несанкціонований доступ до чутливих зон або крадіжка пристроїв, що містять конфіденційну інформацію, можуть поставити під загрозу безпеку.

12. *Атаки «людина посередині»*. У цьому типі атак зловмисник перехоплює комунікацію між двома сторонами і потенційно може підслуховувати, змінювати або впроваджувати шкідливий вміст у комунікацію.

13. *Атаки на відмову в обслуговуванні* (DoS-атаки) мають на меті порушити доступність систем або сервісів, перевантажуючи їх надмірним трафіком, роблячи їх недоступними для законних користувачів.

14. Зберігання або передача конфіденційної *інформації без шифрування* може призвести до її перехоплення та несанкціонованого доступу.

1. Недостатня обізнаність про безпеку: Недостатня обізнаність користувачів з найкращими практиками безпеки, такими як виявлення спроб фішингу або уникнення підозрілих завантажень, може збільшити ризик інцидентів, пов'язаних з безпекою.

Огляд міжнародних і галузевих стандартів з інформаційної безпеки

Для розробки практичної складової навчальних та удосконалення переліку компетенцій треба враховувати актуальні стандарти, фреймворки та кращі світові та галузеві практики. Для цього в табл. 2 приведені кращі стандарти та практики.

Таблиця 2

Перелік міжнародних і галузевих стандартів у сфері інформаційної безпеки

Стандарт	Уточнення	Короткий опис	Сфера застосування	Сфери уваги
ISO/IEC 19788 [6]	—	Стандарт для навчання, освіти та тренінгів з ІБ	Тренінг з ІБ	Розробка навчальних програм, навчальні процеси
NIST Cybersecurity Framework [7]	National Institute of Standards and Technology Cybersecurity Framework	Рамки для управління та покращення стану кібербезпеки	Управління кібербезпекою	Ідентифікувати, захищати, виявляти, реагувати, відновлювати інформаційні системи
FISMA [8]	Federal Information Security Management Act	Федеральний закон США про захист інформаційних систем федерального уряду	Державна ІБ	Управління ризиками, контроль безпеки, комплаєнс
FedRAMP [9]	Federal Risk and Authorization Management Program	Урядова програма США	Стандартизований підхід до оцінки безпеки, авторизації та постійного моніторингу хмарних служб	Державна кібербезпека або хмарна безпека
ANSI/ISA-62443 [10]	—	Розроблені Міжнародним товариством автоматизації (ISA) для безпеці систем промислової автоматизації та управління (IACS)	Безпека промислових систем управління у виробництві, енергетиці та транспорті	Забезпечення безпеки критичної інфраструктури, оцінка ризиків, контроль безпеки
PCI DSS [11]	Payment Card Industry Data Security Standard	Стандарт безпеки для захисту даних кредитних карток	Захист даних платіжних карток	Безпека даних, шифрування, контроль доступу

SWIFT CSP [12]	Society for Worldwide Interbank Financial Telecommunication Customer Security Programme	Забезпечення вузькоспеціалізованого обміну SWIFT-повідомленнями	Безпека систем обміну фінансовими повідомленнями, які використовуються банками та фінансовими установами	Фінансова індустрія
GDPR [13]	General Data Protection Regulation	Регламент Європейського Союзу про захист персональних даних	Захист персональних даних	Конфіденційність даних, згода, підзвітність
HIPAA [14]	Health Insurance Portability and Accountability Act	Стандарт захисту конфіденційної медичної інформації	Захист медичних даних	Конфіденційність, контроль безпеки, сповіщення про порушення
COBIT [15]	Control Objectives for Information and Related Technologies	Структура управління та менеджменту корпоративної інформації та технологій	Управління та контроль над інформаційними системами	IT-процеси, управління ризиками, комплаєнс
SOC 2 [16]	Service Organization Control 2	Розроблено Американським інститутом CPA (AICPA)	Структура для оцінки та звітування про безпеку, доступність, цілісність обробки, конфіденційність і контроль конфіденційності обслуговуючих організацій	Хмарні обчислення та безпека постачальників послуг
BSI Standards [17]	IT-Grundschutz	Розроблений Федеральним відомством з ІБ Німеччини (BSI)	Впровадження ІБ в організаціях	Принципи та заходи щодо оцінки ризиків, управління ризиками та впровадження контролю безпеки
ISO/IEC 15408 Common Criteria [18]	—	Стандарт для оцінки та сертифікації безпеки IT-продуктів і систем	Визначення вимог безпеки та проведення незалежного оцінювання	Загальних критеріїв та її застосування в сертифікації безпеки
CIS Controls [19]	Center for Internet Security Controls	Пріоритетні найкращі практики для захисту систем і даних	Безпека системи та даних	Контроль безпеки, управління ризиками
ISO/IEC 27002 [20]	Раніше ISO/IEC 17799	Кодекс практики управління ІБ	Контроль ІБ	Політика безпеки, контроль, управління ризиками
ISO/IEC 19790 [21]	—	Стандарт щодо вимог безпеки для криптографічних модулів	Безпека криптографічного модуля	Вимоги безпеки, сертифікація модулів

ISO/IEC 20001 [22]	—	Стандарт для системи управління IT-послугами (ITSMS)	Управління IT-послугами	Розробка сервісу, перехід, експлуатація
ISO/IEC 27001 [23]	—	Міжнародний стандарт для системи управління ІБ	Управління ІБ	Оцінка ризиків, засоби контролю, структура системи управління ІБ
ISO/IEC 27005 [24]	—	Стандарт управління ризиками ІБ	Управління ризиками ІБ	Оцінка та моніторинг ризиків
ISO/IEC 27701 [25]	—	Стандарт для систем управління інформацією про конфіденційність	Управління конфіденційністю	Конфіденційність даних, комплаєнс, управління ризиками
ISO/IEC 29151 [26]	—	Стандарт для системи забезпечення конфіденційності персональних даних у хмарі	Структура конфіденційності для хмари	Конфіденційність даних у хмарних середовищах
ISO/IEC 38505-1 [27]	—	Керівництво з управління інвестиціями за допомогою IT	Управління інвестиціями за допомогою IT	Прийняття рішень, управління вартістю та ризиками
FIPS [28]	Federal Information Processing Standards	Видається Національним інститутом стандартів і технологій (NIST) у США	Різні аспекти ІБ	Криптографічні алгоритми (FIPS 140-2) і безпечне знищення даних (FIPS 800-88)
OWASP [29]	Open Web Application Security Project	Не є стандартом у традиційному розумінні, він надає велику кількість ресурсів і вказівок	Безпека веб-додатків	OWASP Top Ten, який висвітлює найбільш критичні ризики безпеки веб-додатків

Комплексний підхід при формуванні навчальних програм потребує комбінації стандартів. Для прикладу взятий стандарт для спеціальності 125 «Кібербезпека» [30] та показаний зв’язок з вищезгаданими стандартами (див. табл. 3).

Таблиця 3

Покриття стандартами компетенцій другого рівня програми 125 «Кібербезпека»

Шифр	**Компетенція**	**Стандарти, які покривають компетенції**
КЗ-1	Застосовувати знання у **практичних** ситуаціях	NIST Cybersecurity Framework
КЗ-2	Проводити **дослідження** на відповідному рівні	ISO/IEC 19788
КЗ-3	**Абстрактне мислення**, **аналіз** та **синтез**	FISMA, COBIT, BSI Standards, ISO/IEC 27005, ISO/IEC 27701
КЗ-4	Оцінювати та забезпечувати **якість** виконуваних **робіт**	ISO/IEC 38505-1, ISO/IEC 20001, ISO/IEC 27002, BSI Standards

КЗ-5	Спілкуватися з представниками інших **професійних груп** різного рівня	GDPR, HIPAA
КФ-1	Обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати **сучасні інформаційні технології**, фізичні та математичні моделі, а також технології створення та використання **прикладного** і **спеціалізованого програмного забезпечення** для вирішення професійних задач у сфері ІБ та/або кібербезпеки	ISO/IEC 19788, OWASP
КФ-2	Розробляти, впроваджувати та аналізувати **нормативні документи**, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати **кращі світові практики**, **стандарти** у професійній діяльності в сфері ІБ та/або кібербезпеки	ISO/IEC 15408 Common Criteria, ANSI/ISA-62443, ISO/IEC 20001, ISO/IEC 27002, CIS Controls, NIST Cybersecurity Framework
КФ-3	Досліджувати, розробляти і супроводжувати методи та засоби ІБ та/або кібербезпеки на **об'єктах інформаційної діяльності** та **критичної інфраструктури**	FISMA, ANSI/ISA-62443, FedRAMP
КФ-4	Аналізувати, розробляти і супроводжувати **систему управління ІБ** та/або кібербезпекою організації, формувати стратегію і **політики ІБ** з урахуванням вітчизняних і міжнародних стандартів та вимог	ISO/IEC 27001, ISO/IEC 15408 Common Criteria
КФ-5	Дослідження, системний аналіз та забезпечення **безперервності бізнес/операційних процесів** з метою визначення вразливостей інформаційних систем та ресурсів, **аналізу ризиків** та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики ІБ та/або кібербезпеки організації	FISMA, COBIT, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 38505-1
КФ-6	Аналізувати, контролювати та забезпечувати **систему управління доступом** до інформаційних ресурсів згідно встановленої стратегії і політики ІБ та/або кібербезпеки організації	ISO/IEC 29151, PCI DSS
КФ-7	Досліджувати, розробляти та впроваджувати методи і заходи **протидії кіберінцидентам**, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо **попередження** та **аналізу кіберінцидентів** в цілому	ISO/IEC 27001, ISO/IEC 27701
КФ-8	Досліджувати, розробляти, впроваджувати та супроводжувати методи і **засоби криптографічного та технічного захисту** інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики ІБ та/або кібербезпеки організації	FIPS, ANSI/ISA-62443, ISO/IEC 19790, PCI DSS
КФ-9	Аналізувати, розробляти і супроводжувати систему **аудиту** та **моніторингу ефективності функціонування** інформаційних систем і технологій, бізнес/операційних процесів в галузі ІБ та/або кібербезпеки організації в цілому	COBIT, SOC 2, BSI Standards, ANSI/ISA-62443
КФ-10	Провадити **науково-педагогічну діяльність**, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань ІБ та/або кібербезпеки	ISO/IEC 19788
КФ-11	Здійснювати **наукові** та/або **прикладні дослідження** у галузі ІБ та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність	ISO/IEC 19788

Так як кілька стандартів покривають різні компетенції, то наочно можна представити ці зв'язки для загальних (рис. 1) та спеціальних (фахових) компетентностей (рис. 2).

ISSN 2663 - 4023

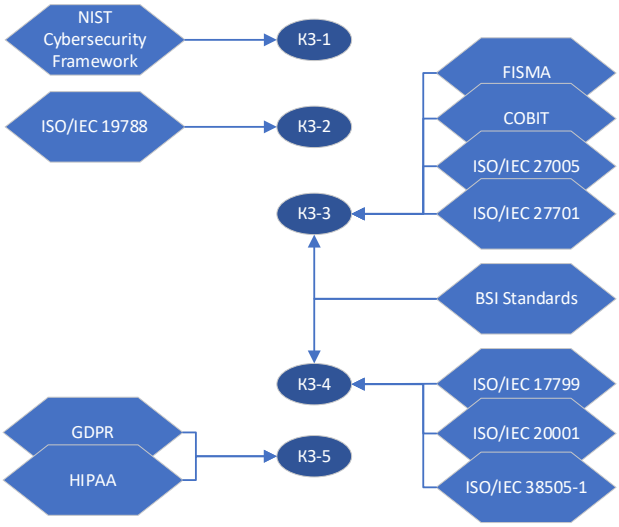

Рис. 1. Зв'язок загальних компетентностей із стандартами безпеки

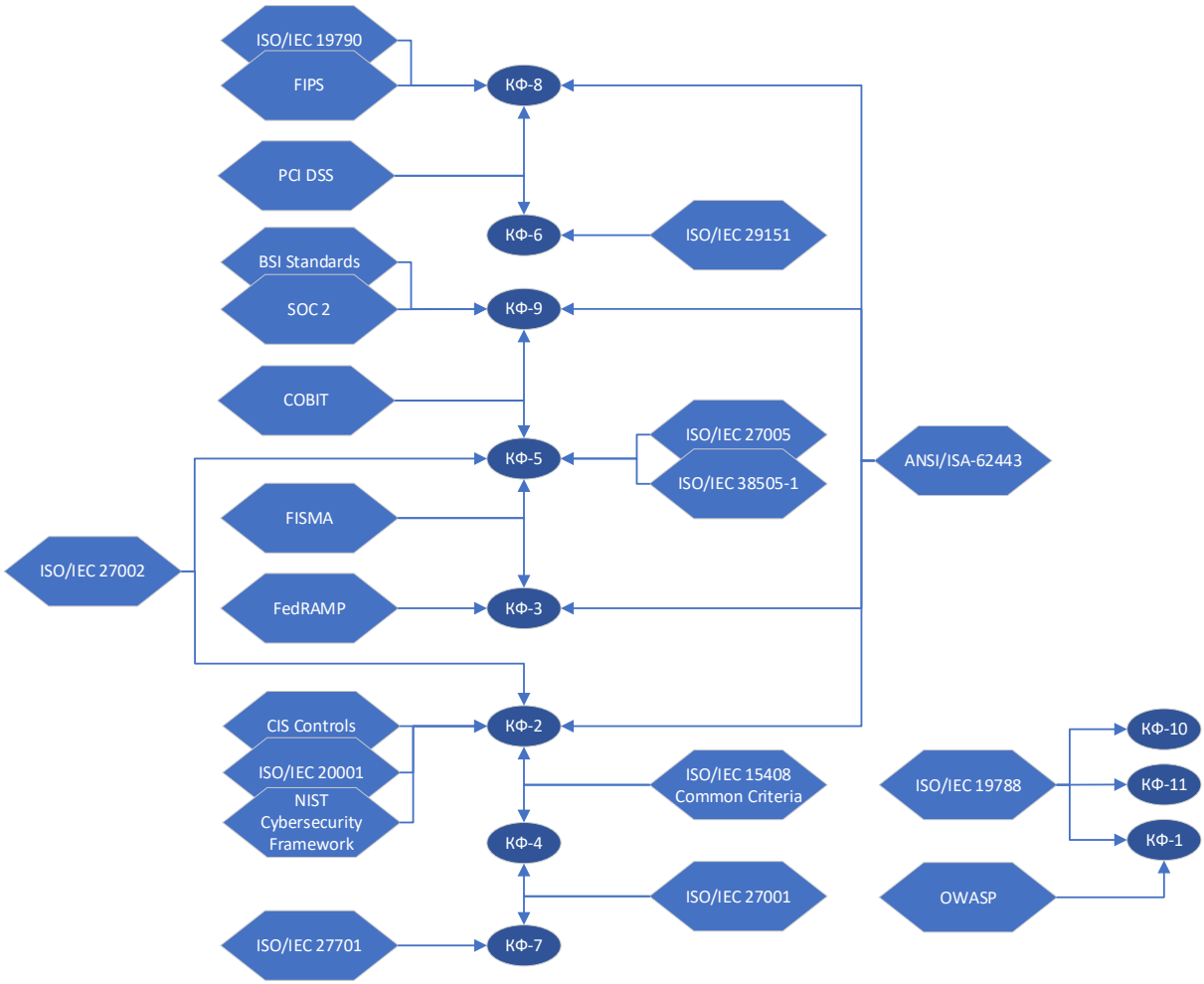

Рис. 2. Зв'язок спеціальних компетентностей із стандартами безпеки

Як видно з рис. 1 і 2, стандарти для різних типів компетенцій перетинаються, що дозволяє здобувачу освіти скласти комплексний підхід до сучасних технік по забезпеченню безпеки.

Порівняльний аналіз рівнів вищої освіти для спеціаліста з кібербезпеки

Для різних освітній рівнів постають різні виклики. Складність з рівнем підвищується, тому пропущені знання на нижчих рівнях призводять до різкого збільшення навантаження для закриття прогалин у знаннях. Табл. 4 покриває основні вимоги до формування спеціалістів на різних рівнях.

Таблиця 4

Порівняння вимог освітнього стандарту з кібербезпеки для першого, другого та третього освітнього рівня

Вимоги	**Перший рівень [31]**	**Другий рівень**	**Третій рівень**
Фундаментальні знання	Всебічне розуміння основних концепцій та принципі	Глибокі знання та досвід	Володіння теоріями та концепціями сучасної ІБ
Технічні навички	Компетентність у впровадженні та управлінні засобами контролю безпеки, технологіями та інструментами	Високий рівень володіння технічними навичками, включаючи безпечний дизайн мережі, реагування на інциденти та управління ризиками	Високий рівень технічної експертизи та здатність проводити оригінальні дослідження у спеціалізованих сферах кібербезпеки
Практичний досвід	Практичне застосування навичок через проєкти, стажування або досвід спільного навчання.	Можливості для отримання практичного досвіду в реальних сценаріях та галузевих партнерствах	Значний практичний досвід завдяки дослідницьким проектам, співпраці з промисловістю та академічними колами та викладання
Оцінка та управління ризиками	Розуміння методологій оцінки ризиків та вміння виявляти та аналізувати ризики	Вміння проводити оцінку ризиків, розробляти стратегії зменшення ризиків та застосовувати системи управління ризиками	Поглиблені навички аналізу та управління складними ризиками, включаючи стратегічне планування ризиків та прийняття рішень
Реагування на інциденти та криміналістика	Володіння процедурами реагування на інциденти, включаючи виявлення, локалізацію, розслідування та відновлення інцидентів	Поглиблені знання та досвід у плануванні, виконанні та координації реагування на інциденти	Експертиза в управлінні реагуванням на інциденти, включаючи розробку інноваційних підходів та дослідження
Управління безпекою та комплаєнс	Ознайомлення з системами управління кібербезпекою та найкращими практиками	Розуміння правових, регуляторних та комплаєнс-вимог	Досвід розробки та впровадження комплексних систем управління безпекою відповідних норм і стандартів
Етична та професійна поведінка	Дотримання етичних стандартів та професійних кодексів поведінки	Продовження розвитку етичної та професійної поведінки	Високі етичні стандарти, лідерство у просуванні етичної

			поведінки та внесок у професійну спільноту
Дослідження та інновації	Обмежене залучення до досліджень; ознайомлення з дослідницькими концепціями	Можливості для науково-дослідницьких проектів та залучення до передових досліджень	Активна участь у дослідженнях, включаючи оригінальні наукові роботи, публікації та просування знань
Безперервне навчання та професійний розвиток	Прихильність до безперервного навчання та постійного ознайомлення з останніми розробками, тенденціями та загрозами	Акцент на безперервному навчанні та професійному розвитку через сертифікати, конференції та семінари	Постійне прагнення до знань та професійного розвитку, що сприяє розвитку кібербезпеки як дисципліни

Якщо порівняти другий (магістранти) та третій (аспіранти й ад'юнкти) освітні рівні, на яких здобувачі отримують не тільки практичні навички (див. табл. 5), але і основи наукової діяльності, то видно, що на обох рівнях потрібне направлення та рецензування більш досвідчених науковців:

• консультації та критика співробітників наукової чи науко-освітньої установи, інших суміжних установ;

• міжнародні контакти;

• спілкування з авторами публікацій за темою дослідження через наукові соціальні мережі або напряму по електронній пошті.

Таблиця 5

Порівняльний аналіз підходів до навчання другого та третього освітнього рівня

Аспект дослідження	**Другий рівень**	**Третій рівень**
Обсяг	Часто вужчі за обсягом, зосереджені на практичному застосуванні або конкретних методах у сфері ІБ.	Охоплює ширші або міждисциплінарні аспекти, включаючи теоретичні рамки, політичні наслідки або розробку нових методик
Глибина	Як правило, зосереджені на конкретній сфері ІБ, забезпечуючи всебічне розуміння обраної теми	Передбачає більш спеціалізовані та поглиблені дослідження, що сприяють поглибленню знань у певній підгалузі або вирішенню нових викликів
Методологічна строгість	Акцент на набутті практичних навичок та застосуванні усталених методів дослідження для вивчення конкретних безпекових викликів	Очікується, що кандидат продемонструє глибоке розуміння методології досліджень, включаючи ретельний експериментальний дизайн, статистичний аналіз та критичну оцінку існуючих підходів
Незалежність	Зазвичай під наглядом або під керівництвом радника чи наставника, з регулярними перевірками та настановами протягом усього проекту	Очікується вищий рівень незалежності та відповідальності, рідше здійснюється нагляд, реалізацію та прийняття рішень щодо проєктів
Внесок	Очікується, що здобувачі зроблять внесок в існуючу базу знань, досліджуючи або застосовуючи існуючі концепції, методології або методи	Очікується, що здобувачі зроблять значний внесок у галузь, наприклад, запропонують нові теорії, інноваційні рішення або вдосконалять методологію
Публікаційний потенціал	Хоча публікації в академічних журналах або на конференціях	Заохочуємо шукати можливості для публікацій, щоб поширювати

	заохочуються, здобувачі можуть бути менш поширеними порівняно з аспірантами	результати досліджень і робити внесок в академічну спільноту. Високо цінуються публікації в авторитетних виданнях
Часові рамки	Зазвичай завершується в межах визначеного терміну магістерської програми (від одного до двох років)	Може виходити за межі визначеної тривалості програми, надаючи більше часу для всебічних досліджень та експериментів

В залежності від освітнього рівня висуваються різні вимоги до широти дослідження. В табл. 6 представлені етапи формалізованого представлення дослідження, але не всі вони обов'язкові для різних рівнів.

Таблиця 6

Етапи представлення результатів звіту про наукове дослідження

Етап	Назва	Опис	Обов'язковість для	
			Другого рівня	Третього рівня
1	Тема	Тема дослідження або проблема, яку необхідно вирішити	Так	Так
2	Мета	Конкретна мета або завдання дослідження	Так	Так
3	Актуальность	Актуальність, новизна та обмеження дослідження	Так	Так
4	Огляд літератури	Проведення всебічного огляду існуючої літератури, пов'язаної з даною темою	Ні	Так
5	Питання дослідження	Формулювання конкретних дослідницьких запитань для спрямування дослідження	Ні	Ні
6	Методологія	Опис методології дослідження та методів збору даних, які будуть використані	Ні	Так
7	Аналіз даних	Аналіз зібраних даних за допомогою відповідних методик	Так	Так
8	Результати	Представлення висновків та результатів дослідження	Так	Так
9	Обговорення	Інтерпретація та обговорення результатів відповідно до питань дослідження	Ні	Ні
10	Висновок	Підсумовуючи основні висновки та їх наслідки	Так	Так
11	Вдячність	За критику, фінансування або поради	Ні	Ні
12	Посилання	Посилання на інформаційні джерела	Так	Так
13	Обмеження використання	Секретність інформації, захищеної авторським правом, або обмеженнями законодавства	Ні	Ні

Відмінності у навчальних програмах з ІБ для студентів та аспірантів:

1. *Глибина та складність змісту*. Навчальні програми аспірантури, як правило, заглиблюються в складні концепції, теорії та дослідження в галузі ІБ. Зміст може бути більш складним і охоплювати такі теми, як криптографія, розширена мережева безпека, архітектура безпеки та нові технології. Бакалаврські програми, з іншого боку, можуть надавати ширший вступ до принципів ІБ та фундаментальних знань.

2. *Дослідницький фокус*. Аспірантські програми часто роблять акцент на дослідженнях і заохочують студентів робити свій внесок у цю сферу за допомогою оригінальних дослідницьких проектів або дисертаційних робіт. Це передбачає розробку дослідницьких методологій, проведення поглибленого аналізу та внесок у розвиток знань у конкретних сферах ІБ. Бакалаврські програми можуть мати обмежені дослідницькі можливості або зосереджуватися більше на розвитку практичних навичок.

3. *Практичні навички та досвід*. Як бакалаврські, так і магістерські програми повинні включати практичні вправи та реальні сценарії для закріплення теоретичних концепцій. Однак, програми післядипломної освіти можуть приділяти більше уваги поглибленим технічним навичкам, таким як тестування на проникнення, реагування на інциденти та аналіз безпеки, щоб підготувати студентів до більш спеціалізованих ролей або кар'єри, орієнтованої на дослідницьку діяльність.

4. *Широта знань*. Бакалаврські програми часто охоплюють ширший спектр тем з ІБ, щоб забезпечити всебічне розуміння галузі. Сюди входять такі сфери, як мережева безпека, безпека додатків, управління безпекою, оцінка ризиків, а також правові та етичні міркування. Аспірантські програми можуть передбачати більшу спеціалізацію, що дозволяє студентам зосередитися на конкретних сферах, які їх цікавлять в ІБ.

5. *Професійний розвиток та лідерство*. Аспірантські програми можуть включати компоненти, які зосереджені на розвитку лідерських навичок, управлінських здібностей та розумінні прийняття стратегічних рішень в контексті ІБ. Це готує студентів до керівних посад або управлінських ролей в організаціях, де вони можуть відповідати за нагляд за програмами та ініціативами з ІБ.

6. *Можливості співпраці та нетворкінгу*. Аспірантські програми часто пропонують більше можливостей для співпраці з колегами, викладачами та професіоналами галузі. Ці програми сприяють проведенню нетворкінгових заходів, запрошених лекцій, конференцій та галузевих партнерств, що дозволяє студентам встановлювати цінні зв'язки та брати участь в обміні знаннями в рамках спільноти ІБ.

7. *Передумови та вимоги до вступу*. Програми післядипломної освіти, як правило, мають суворіші вимоги до вступників, включаючи ступінь бакалавра у спорідненій галузі, а іноді й відповідний досвід роботи. Бакалаврські програми, з іншого боку, розраховані на студентів з різним досвідом і можуть не мати спеціальних вимог, окрім загальних вимог до вступу.

Комплексне формування навичок у здобувачів вищої освіти

Успіх фахівця з ІБ може визначатися набором навичок, представленим в табл. 7.

Таблиця 7

Конкурентні засади для формування спеціаліста з кібербезпеки

Навичка	**Опис**
Знання та досвід	Володіння міцним фундаментом знань і досвіду в галузі ІБ має вирішальне значення. Це включає в себе розуміння різних концепцій безпеки, технологій, найкращих практик, нормативних актів та галузевих стандартів. Безперервне навчання та постійне ознайомлення з останніми досягненнями в цій галузі також є дуже важливими
Технічні навички	Фахівці з ІБ повинні мати глибоке розуміння технічних аспектів, пов'язаних з мережами, системами, додатками, криптографією, оцінкою вразливостей, тестуванням на проникнення, реагуванням на інциденти та іншими відповідними сферами. Вміння використовувати інструменти та технології безпеки є надзвичайно цінним
Здатність вирішувати проблеми	Успіх у сфері ІБ вимагає вміння аналізувати складні проблеми, виявляти вразливості та розробляти ефективні рішення. Фахівці з ІБ повинні володіти навичками критичного мислення, оцінки ризиків та методологіями вирішення проблем, щоб ефективно протистояти викликам безпеки

Адаптивність та постійне вдосконалення	Сфера ІБ динамічна і постійно розвивається. Успішні фахівці повинні бути адаптивними, гнучкими та відкритими до вивчення нових технологій і підходів. Вони повинні активно шукати можливості для професійного розвитку, брати участь у конференціях, навчальних програмах та відвідувати галузеві форуми, щоб залишатися в курсі подій
Етична та професійна поведінка	Демонстрація етичної поведінки та дотримання професійних стандартів має вирішальне значення у сфері ІБ. Дотримання конфіденційності, доброчесність і професіоналізм є важливими рисами для побудови довіри з клієнтами, колегами та зацікавленими сторонами
Комунікативні навички	Сильні комунікативні навички, як усні, так і письмові, є життєво важливими для фахівця з ІБ. Вони повинні вміти ефективно доносити технічні концепції до нетехнічних зацікавлених сторін, писати чіткі звіти та формулювати рекомендації або висновки щодо безпеки для керівництва або клієнтів
Співпраця та командна робота	ІБ нечасто буває справою самотньої людини. Успіх часто вимагає співпраці з командами або іншими фахівцями в організації. Здатність ефективно працювати в команді, співпрацювати з міжфункціональними відділами та брати участь в обміні знаннями є запорукою успіху
Результати та вплив	Зрештою, успіх фахівця з ІБ можна виміряти за його здатністю захищати критичні активи організації, зменшувати ризики та сприяти покращенню загального стану безпеки. Здатність досягати відчутних результатів і позитивно впливати на середовище безпеки організації є важливим показником успіху

Списки компетенцій навчальних програм мають відповідати представленому списку навичок.

Вимоги до освітнього стандарту для підготовки фахівців з кібербезпеки

За результатами розгляду та порівняння кращих існуючих практик та стандартів можна виділити вимоги до компетенцій фахівців другого освітнього рівня:

1. *Розширені знання з ІБ*. Всебічне розуміння фундаментальних понять та принципів кібербезпеки. Досвід роботи в різних сферах кібербезпеки, включаючи мережеву безпеку [32] – [34], безпеку додатків [35], безпеку даних, реагування на інциденти, управління ризиками та управління.

2. *Технічні навички*. Компетентність у впровадженні та управлінні засобами контролю безпеки, технологіями та інструментами, що використовуються в кібербезпеці. Досвід проведення оцінки вразливостей, тестування на проникнення [36] та аудиту безпеки [37]. Знання практик безпечного кодування, криптографії [38], безпечних мережевих архітектур [39] – [41] та методологій розробки безпечного програмного забезпечення [42]. Вміння налаштовувати та керувати інфраструктурою безпеки, наприклад, брандмауерами, системами виявлення та запобігання вторгненням, а також системами управління інформацією та подіями безпеки (SIEM).

3. *Управління ризиками*. Розуміння методологій оцінки ризиків та вміння виявляти та аналізувати ризики кібербезпеки. Знання систем управління ризиками та практик для розробки стратегій зменшення ризиків. Здатність оцінювати вплив ризиків кібербезпеки на цілі організації та розробляти плани протидії ризикам.

4. *Реагування на інциденти та криміналістика*. Володіння процедурами реагування на інциденти, включаючи виявлення та інформування про спроби соціального інжинірингу [43] – [45], локалізацію, розслідування та відновлення інцидентів. Знання принципів і методів цифрової криміналістики для збору та аналізу доказів. Здатність розробляти плани реагування на інциденти та координувати зусилля з реагування на інциденти.

5. *Управління безпекою та комплаєнс*. Ознайомлення з системами управління кібербезпекою та найкращими практиками. Розуміння правових, регуляторних та

комплаєнс-вимог, що стосуються кібербезпеки, таких як GDPR, HIPAA та PCI DSS. Знання політик, стандартів і процедур безпеки та вміння розробляти і впроваджувати їх в організаціях.

6. *Етична та професійна поведінка*. Дотримання етичних стандартів та професійних кодексів поведінки у сфері кібербезпеки. Усвідомлення правових та етичних наслідків дій та рішень у сфері кібербезпеки. Здатність ефективно спілкуватися, співпрацювати та демонструвати професіоналізм у сфері кібербезпеки.

7. *Дослідження та інновації*. Здатність проводити дослідження в галузі кібербезпеки, сприяти поглибленню знань у цій сфері та застосовувати результати досліджень до реальних сценаріїв. Вміння оцінювати нові тенденції, технології та загрози у сфері кібербезпеки та адаптувати стратегії відповідно до них, наприклад, при роботі з кіберполігонами та іншими віртуальними ізольованими середовищами для дослідження реальних загроз [46].

8. *Досвід*. Практичне застосування навичок кібербезпеки через практичні проекти, стажування або досвід спільного навчання. Можливість працювати з професіоналами галузі, брати участь у змаганнях з кібербезпеки або вирішувати реальні проблеми кібербезпеки.

9. *Безперервне навчання та професійний розвиток*. Прихильність до безперервного навчання та постійного ознайомлення з останніми розробками, тенденціями та загрозами у сфері кібербезпеки. Можливості для професійного розвитку, такі як відвідування конференцій, семінарів та навчальних програм.

Слід зазначити, що для третього освітнього рівня даний перелік розширяється наукової складовою та публічним представлення кінцевих результатів дослідження. Всі перелічені вимоги мають бути побудовані в практичній площині, наприклад, за допомогою CDIO підходів [47] та гнучких методів навчання [48].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті проаналізований світовий ринок з надання освітніх послуг в сфері інформаційної безпеки та кібербезпеки. Видно, що одночасно відбуваються два процеси: перехід від практичних навичок до фундаментальних знань і навпаки. Найуспішнішими є ті заклади вищої освіти, які можуть комбінувати обидва підходи одночасно. Але для цього потрібно мати в своєму складі експериментальну базу, практичні навчальні лабораторії та штат викладачів і науковців. Таку задачу можуть виконувати лише великі установи.

Так як виклики в кібербезпеці постійно змінюються, то від закладів вищої освіти вимагається вдосконалювати свої програми щорічно. Одночасно з процесом оновлення підходів до викладання проходять процеси вдосконалення корпусі міжнародних та галузевих стандартів, а також різноманітних кращих практик та фреймворків. Швидка зміна вимагає не тільки від викладачів постійного вдосконалення, але і від практикуючих фахівців з кібербезпеки. Таким чином, процес постійного навчання має продовжуватися й після формального закінчення магістратури чи аспірантури.

В результаті даного дослідження видно, що лише комплексне формування навичок з інформаційної безпеки дозволяє якісно підготувати фахівців. На базі цього приведені вимоги до освітнього стандарту для підготовки спеціалістів та науковців.

Подальші дослідження спрямовані на формування стандарту вищої освіти зі спеціальності «Кібербезпека» для третього освітнього рівня.

ПОДЯКА

Автор даної публікації висловлює подяку Володимиру Леонідовичу Бурячку, завідувачу кафедри інформаційної та кібернетичної безпеки (Державний університет телекомунікацій та Київський університет імені Бориса Грінченка), який був безпосереднім керівником і впроваджувачем інноваційних методів в навчанні, а також активно надихав і залучав студентів до наукової роботи [49] – [51].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Соколов, В. (2022). Підходи до формування наукового мислення у здобувачів вищої освіти з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, *2*(*18*), 124–137. https://doi.org/10.28925/2663-4023.2022.18.124137
2 Бурячок, В., *та ін.* (2021). Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень*: Кібербезпека: освіта, наука, техніка*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165
3 Шевченко, С., *та ін.* (2020). Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека. *Кібербезпека: освіта, наука, техніка*, *2*(*10*), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168
4 Бурячок, В., *та ін.* (2020). Застосування середовища Ni Multisim при формуванні практичних навичок студентів спеціальності 125 «Кібербезпека». *Кібербезпека: освіта, наука, техніка*, *1*(*9*), 159–169. https://doi.org/10.28925/2663-4023.2020.9.159169
5 Buriachok, V., *et al.* (2018). Training Model for Professionals in the Field of Information and Cyber Security in the Higher Educational Institutions of Ukraine. *Information Technologies and Learning Tools*, *67*(*5*), 277–291. https://doi.org/10.33407/itlt.v67i5.2347
6 International Organization for Standardization (2020). ISO/IEC 19788-1:2011. Information Technology. Learning, Education and Training. Metadata for Learning Resources. Part 1: Framework. https://www.iso.org/standard/50772.html
7 National Institute of Standards and Technology (2023). Discussion Draft of the NIST Cybersecurity Framework 2.0 Core https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
8 Cybersecurity and Infrastructure Security Agency (2023). FY 2023. Inspector General Federal Information Security Modernization Act of 2014 (FISMA). Metrics Evaluator's Guide, ver. 3.0. https://www.cisa.gov/sites/default/files/2023-05/fy_2023_ig_fisma_metrics_evaluation_guide.pdf
9 FedRAMP (2018). General Document Acceptance Criteria, ver. 2.1. https://www.fedramp.gov/assets/resources/documents/FedRAMP_General_Document_Acceptance_Criteria.pdf
10 International Society of Automation (2020). ISA/IEC 62443. Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
11 PCI Security Standards Council (2022). PCI DSS, ver. 4.0. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
12 Swift (2023). Customer Security Programme. https://www.swift.com/ru/node/300751
13 The European Parliament and of the Council (2018). Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
14 U.S. Department of Health and Human Services Office for Civil Rights (2013). HIPAA Administrative Simplification. Regulation Text. 45 CFR Parts 160, 162, and 164. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
15 Lepofsky, R. (2014). COBIT 5 for Information Security. In: The Manager's Guide to Web Application Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-0148-0_10

16 Association of International Certified Professional Accountants (2023). SOC for Cybersecurity. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity
17 Wollinger, G. R., Schulze, A. (2020). Handbuch Cybersecurity für die öffentliche Verwaltung. KSV Verwaltungspraxis. https://doi.org/10.5771/9783748912057
18 Common Criteria (2022). Common Methodology for Information Technology Security Evaluation. Evaluation Methodology, rev. 1. https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf
19 Center for Internet Security (2023). CIS Critical Security Controls, ver. 8. https://www.cisecurity.org/controls/v8_pre
20 International Organization for Standardization (2022). ISO/IEC 27002:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Controls. https://www.iso.org/standard/75652.html
21 International Organization for Standardization (2012). ISO/IEC 19790:2012. Information Technology. Security Techniques. Security Requirements for cryptographic Modules. https://www.iso.org/standard/52906.html
22 International Organization for Standardization (2018). ISO/IEC 20000-1:2018. Information Technology. Service Management. Part 1: Service Management System Requirements. https://www.iso.org/standard/70636.html
23 International Organization for Standardization (2022). ISO/IEC 27001. Information Security Management Systems. https://www.iso.org/standard/27001
24 International Organization for Standardization (2022). ISO/IEC 27005:2022. Information Security, Cybersecurity and Privacy Protection. Guidance on Managing Information Security Risks. https://www.iso.org/standard/80585.html
25 International Organization for Standardization (2019). ISO/IEC 27701:2019. Security Techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management. Requirements and Guidelines. https://www.iso.org/standard/71670.html
26 International Organization for Standardization (2017). ISO/IEC 29151:2017. Information Technology. Security Techniques. Code of Practice for Personally Identifiable Information Protection. https://www.iso.org/standard/62726.html
27 International Organization for Standardization (2017). ISO/IEC 38505-1:2017. Information Technology. Governance of IT. Governance of Data. Part 1: Application of ISO/IEC 38500 to the Governance of Data. https://www.iso.org/standard/56639.html
28 Information Technology Laboratory (2023). Federal Information Processing Standards. https://csrc.nist.gov/publications/fips
29 Open Web Application Security Project (2023). OWASP Security Knowledge Framework. https://owasp.org/www-project-security-knowledge-framework/
30 Міністерство освіти і науки України (2021). Стандарт вищої освіти України. Другий (магістерський) рівень. 12 Інформаційні технології. 125 Кібербезпека, Наказ №332 від 18.03.2021 р. https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx
31 Бурячок, В., *та ін.* (2016). Методичні рекомендації до виконання дипломних робіт освітнього рівня «Бакалавр» студентів галузі знань 1701 «Інформаційна безпека», ДУТ, НАУ.
32 Yevdokymenko, M., Sokolov, V. (2019). Overview of the Course in “Wireless and Mobile Security.” *Educating the Next Generation MSc in Cyber Security*, 104–119. https://doi.org/10.5281/zenodo.2647747
33 Владимиренко, М., Соколов, В., Астапеня, В. (2019). Дослідження стійкості роботи однорангових безпроводових мереж із самоорганізацією. *Кібербезпека: освіта, наука, техніка*, *3*, 6–26. https://doi.org/10.28925/2663-4023.2019.3.626
34 Taj Dini, M., Sokolov, V. (2017). Internet of Things Security Problems. *Сучасний захист інформації*, *1*, 120–127.
35 Жданова, Ю., Спасітєлєва, С., Шевченко, С., Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 4(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453
36 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Сучасний захист інформації*, *1*, 82–89.
37 Kipchuk, F., *et al.* (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology* (pp. 213–217). https://doi.org/10.1109/picst54195.2021.9772181

38 Курбанмурадов, Д., Соколов, В., Астапеня, В. (2019). Реалізація протоколу шифрування XTEA на базі безпроводових систем стандарту IEEE 802.15.4. *Кібербезпека: освіта, наука, техніка*, *2*(*6*), 32–45. https://doi.org/10.28925/2663-4023.2019.6.3245

39 TajDini, M., Sokolov, V., Buriachok, V. (2019). Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. In *8th International Conference on "Mathematics. Information Technologies. Education,"* 287–296.

40 Buriachok, V., Sokolov, V., Taj Dini, M. (2020). Research of Caller ID Spoofing Launch, Detection, and Defense. *Cybersecurity: Education, Science, Technique*, *1*(*7*), 6–16. https://doi.org/10.28925/2663-4023.2020.7.616

41 TajDini, M., Sokolov, V., Skladannyi, P. (2021). Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics*, 7–11. https://doi.org/10.1109/ukrmico52950.2021.9716665

42 Цирканюк, Д., *et al.* (2021). Метод побудови профілів користувача маркетплейсу і зловмисника. *Кібербезпека: освіта, наука, техніка*, *2*(*14*), 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067

43 Соколов, В., Курбанмурадов Д. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

44 Marusenko, R., Sokolov, V., Buriachok, V. (2020). Experimental Evaluation of Phishing Attack on High School Students. *Advances in Computer Science for Engineering and Education III*, *1247*, 668–680. https://doi.org/10.1007/978-3-030-55506-1_59

45 Marusenko, R., Sokolov, V., Bogachuk, I. (2022). Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation. *Advances in Artificial Systems for Logistics Engineering*, *135*, 583–594. https://doi.org/10.1007/978-3-031-04809-8_53

46 Vyshnivskyi, V., Sokolov, V. (2018). Laboratory Complex "Cyber Range". *Сучасний захист інформації*, 2, 105–107.

47 CDIO office (2019). Ініціатива CDIO (В. Соколов, Пер.). КУБГ. http://www.cdio.org/files/CDIO_standards_ua.pdf

48 Delhij, A., van Solingen, R., Wijnands, W. (2019). Керівництво по eduScrum : «Правила гри» (В. Соколов, пер.). КУБГ.

49 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57

50 Buriachok, V, *et al.* (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. *Lecture Notes on Data Engineering and Communications Technologie*, *178*, 533–551. https://doi.org/10.1007/978-3-031-35467-0_32

51 Бурячок, В., Шевченко, С., Складанний, П. (2018). Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. *Кібербезпека: освіта, наука, техніка*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

Volodymyr Y. Sokolov
Ph.D., associate professor
associate professor of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Pavlo M. Skladannyi
Ph.D., associate professor
head of Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

COMPARATIVE ANALYSIS OF STRATEGIES FOR BUILDING SECOND AND THIRD LEVEL OF 125 "CYBER SECURITY" EDUCATIONAL PROGRAMS

Abstract. The article analyzes the global market for the provision of educational services in the field of information security and cybersecurity. The study aims to compare strategies for building curricula for the second and third levels of education for specialties related to information technology, information, and cybersecurity, as well as to formulate recommendations for harmonizing the learning process and international standards. Cybersecurity training programs are becoming outdated too quickly. ISO standards are updated approximately every four years. Also, the standard for the specialty 125 "Cybersecurity" for the third educational level still needs to be finalized. There is a problem of forming a consistent process of introducing the latest approaches and practices into the curriculum. The growth of the information technology market is leading to an increase in the need for cybersecurity specialists. Two processes are taking place simultaneously: the transition from practical skills to fundamental knowledge and vice versa. The most successful higher education institutions are those that can combine both approaches simultaneously. But this requires an experimental base, practical training laboratories, and a staff of teachers and researchers. Only large institutions can perform this task. Since cybersecurity challenges are constantly changing, higher education institutions are required to improve their programs annually. Simultaneously with the process of updating teaching approaches, the body of international and industry standards, as well as various best practices and frameworks, are being improved. Rapid change requires not only continuous improvement from educators but also from cybersecurity practitioners. Thus, the process of continuous learning should continue after the formal completion of a master's or Ph.D. program. The results of this study show that only a comprehensive development of information security skills allows for high-quality training of specialists. Based on this, the requirements for the educational standard for training specialists and scientists are presented.

Keywords: cyber security; informational security; IS; information technology; IT; information protection; vulnerabilities; learning process; educational standard.

REFERENCES

1 Sokolov, V. (2022). Approaches to the Formation of Scientific Thinking in Cybersecurity High School Students. *Cybersecurity: Education, Science, Technique*, *2*(*18*), 124–137. https://doi.org/10.28925/2663-4023.2022.18.124137

2 Buriachok, V., *et al.* (2021). Interdisciplinary Approach to the Development of Risk Management Skills on the basis of Decision-Making Theory. *Cybersecurity: Education, Science, Technique*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

3 Shevchenko, S., *et al.* (2020). Conducting a Swot-Analysis of Information Risk Assessment as a Means of Formation of Practical Skills of Students Specialty 125 Cyber Security. *Cybersecurity: Education, Science, Technique*, *2*(*10*), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168

4 Buriachok, V., *et al*. (2020). Application of Ni Multisim Environment in the Practical Skills Building for Students of 125 "Cybersecurity" Specialty. *Cybersecurity: Education, Science, Technique, 1*(*9*), 159–169. https://doi.org/10.28925/2663-4023.2020.9.159169

5 Buriachok, V., *et al*. (2018). Training Model for Professionals in the Field of Information and Cyber Security in the Higher Educational Institutions of Ukraine. *Information Technologies and Learning Tools, 67*(5), 277–291. https://doi.org/10.33407/itlt.v67i5.2347

6 International Organization for Standardization (2020). ISO/IEC 19788-1:2011. Information Technology. Learning, Education and Training. Metadata for Learning Resources. Part 1: Framework. https://www.iso.org/standard/50772.html

7 National Institute of Standards and Technology (2023). Discussion Draft of the NIST Cybersecurity Framework 2.0 Core https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf

8 Cybersecurity and Infrastructure Security Agency (2023). FY 2023. Inspector General Federal Information Security Modernization Act of 2014 (FISMA). Metrics Evaluator's Guide, ver. 3.0. https://www.cisa.gov/sites/default/files/2023-05/fy_2023_ig_fisma_metrics_evaluation_guide.pdf

9 FedRAMP (2018). General Document Acceptance Criteria, ver. 2.1. https://www.fedramp.gov/assets/resources/documents/FedRAMP_General_Document_Acceptance_Criteria.pdf

10 International Society of Automation (2020). ISA/IEC 62443. Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

11 PCI Security Standards Council (2022). PCI DSS, ver. 4.0. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

12 Swift (2023). Customer Security Programme. https://www.swift.com/ru/node/300751

13 The European Parliament and of the Council (2018). Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

14 U.S. Department of Health and Human Services Office for Civil Rights (2013). HIPAA Administrative Simplification. Regulation Text. 45 CFR Parts 160, 162, and 164. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

15 Lepofsky, R. (2014). COBIT 5 for Information Security. In: The Manager's Guide to Web Application Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-0148-0_10

16 Association of International Certified Professional Accountants (2023). SOC for Cybersecurity. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity

17 Wollinger, G. R., Schulze, A. (2020). Handbuch Cybersecurity für die öffentliche Verwaltung. KSV Verwaltungspraxis. https://doi.org/10.5771/9783748912057

18 Common Criteria (2022). Common Methodology for Information Technology Security Evaluation. Evaluation Methodology, rev. 1. https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf

19 Center for Internet Security (2023). CIS Critical Security Controls, ver. 8. https://www.cisecurity.org/controls/v8_pre

20 International Organization for Standardization (2022). ISO/IEC 27002:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Controls. https://www.iso.org/standard/75652.html

21 International Organization for Standardization (2012). ISO/IEC 19790:2012. Information Technology. Security Techniques. Security Requirements for cryptographic Modules. https://www.iso.org/standard/52906.html

22 International Organization for Standardization (2018). ISO/IEC 20000-1:2018. Information Technology. Service Management. Part 1: Service Management System Requirements. https://www.iso.org/standard/70636.html

23 International Organization for Standardization (2022). ISO/IEC 27001. Information Security Management Systems. https://www.iso.org/standard/27001

24 International Organization for Standardization (2022). ISO/IEC 27005:2022. Information Security, Cybersecurity and Privacy Protection. Guidance on Managing Information Security Risks. https://www.iso.org/standard/80585.html
25 International Organization for Standardization (2019). ISO/IEC 27701:2019. Security Techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management. Requirements and Guidelines. https://www.iso.org/standard/71670.html
26 International Organization for Standardization (2017). ISO/IEC 29151:2017. Information Technology. Security Techniques. Code of Practice for Personally Identifiable Information Protection. https://www.iso.org/standard/62726.html
27 International Organization for Standardization (2017). ISO/IEC 38505-1:2017. Information Technology. Governance of IT. Governance of Data. Part 1: Application of ISO/IEC 38500 to the Governance of Data. https://www.iso.org/standard/56639.html
28 Information Technology Laboratory (2023). Federal Information Processing Standards. https://csrc.nist.gov/publications/fips
29 Open Web Application Security Project (2023). OWASP Security Knowledge Framework. https://owasp.org/www-project-security-knowledge-framework/
30 Ministry of Education and Science of Ukraine (2021). Standard of Higher Education of Ukraine. Second (Master's) Level. 12 Information Technologies. 125 Cybersecurity, No. 332 dated March 18, 2021 https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx
31 Buriachok, V., *et al.* (2016). Methodological Recommendations for the Completion of Diploma Theses of the Educational Level "Bachelor" of Students of the Field of Knowledge 1701 "Information Security," DUT, NAU.
32 Yevdokymenko, M., Sokolov, V. (2019). Overview of the Course in "Wireless and Mobile Security." *Educating the Next Generation MSc in Cyber Security*, 104–119. https://doi.org/10.5281/zenodo.2647747
33 Vladymyrenko, M., Sokolov, V., Astapenia, V. (2019). Study of Stability of Peer-to-Peer Wireless Networks with Self-Organization. *Cybersecurity: Education, Science, Technique*, *3*, 6–26. https://doi.org/10.28925/2663-4023.2019.3.626
34 Taj Dini, M., Sokolov, V. (2017). Internet of Things Security Problems. *Modern Information Protection*, *1*, 120–127.
35 Zhdanova Y., Spasiteleva, S., Shevchenko, S. (2019). Application Of The Security.Cryptography Class Library For Practical Training Of Specialists From The Cyber Security. *Cybersecurity: Education, Science, Technique*, 4(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453
36 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Modern Information Protection*, *1*, 82–89.
37 Kipchuk, F., *et al.* (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology*, 213–217. https://doi.org/10.1109/picst54195.2021.9772181
38 Kurbanmuradov, D., Sokolov, V., Astapenia, V. (2019). Implementation of the XTEA Encryption Protocol based on Wireless Systems of the IEEE 802.15.4 Standard. *Cybersecurity: Education, Science, Technique*, *2*(*6*). 32–45. https://doi.org/10.28925/2663-4023.2019.6.3245
39 TajDini, M., Sokolov, V., Buriachok, V. (2019). Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. In *8th International Conference on "Mathematics. Information Technologies. Education,"* 287–296.
40 Buriachok, V., Sokolov, V., Taj Dini, M. (2020). Research of Caller ID Spoofing Launch, Detection, and Defense. *Cybersecurity: Education, Science, Technique*, *1*(*7*), 6–16. https://doi.org/10.28925/2663-4023.2020.7.616
41 TajDini, M., Sokolov, V., Skladannyi, P. (2021). Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics*, 7–11. https://doi.org/10.1109/ukrmico52950.2021.9716665
42 Tsyrkaniuk, D., *et al.* (2021). Method of Marketplace Legitimate User and Attacker Profiling. *Cybersecurity: Education, Science, Technique*, *2*(*14*), 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067
43 Sokolov, V., Kurbanmuradov D. (2018). The Method of Combating Social Engineering at the Objects of Information Activity. *Cybersecurity: Education, Science, Technique*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

44 Marusenko, R., Sokolov, V., Buriachok, V. (2020). Experimental Evaluation of Phishing Attack on High School Students. *Advances in Computer Science for Engineering and Education III*, *1247*, 668–680. https://doi.org/10.1007/978-3-030-55506-1_59

45 Marusenko, R., Sokolov, V., Bogachuk, I. (2022). Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation. *Advances in Artificial Systems for Logistics Engineering*, *135*, 583–594. https://doi.org/10.1007/978-3-031-04809-8_53

46 Vyshnivskyi, V., Sokolov, V. (2018). Laboratory Complex "Cyber Range." *Modern Information Protection*, 2, 105–107.

47 CDIO Office (2019). CDIO Standards 2.1. http://www.cdio.org/content/cdio-standards-21

48 Delhij, A., van Solingen, R., Wijnands, W. (2015). The eduScrum Guide "The rules of the Game."

49 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57

50 Buriachok, V, *et al.* (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. *Lecture Notes on Data Engineering and Communications Technologie*, *178*, 533–551. https://doi.org/10.1007/978-3-031-35467-0_32

51 Buriachok, V., Shevchenko, S., Skladannyi, P. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104