



DOI [10.28925/2663-4023.2021.11.155165](https://doi.org/10.28925/2663-4023.2021.11.155165)

УДК 004.94:519.21

**Бурячок Володимир Леонідович**

д.т.н., професор,  
завідувач кафедри інформаційної та кібернетичної безпеки  
Київський університет імені Бориса Грінченка, Київ, Україна  
ORCID ID: 0000-0002-4055-1494  
[v.buriachok@kubg.edu.ua](mailto:v.buriachok@kubg.edu.ua)

**Шевченко Світлана Миколаївна**

канд. пед. наук, доцент,  
доцент кафедри інформаційної та кібернетичної безпеки  
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна  
ORCID ID: 0000-0002-9736-8623  
[s.shevchenko@kubg.edu.ua](mailto:s.shevchenko@kubg.edu.ua)

**Жданова Юлія Дмитрівна**

канд. ф.-м. наук, доцент,  
доцент кафедри інформаційної та кібернетичної безпеки  
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна  
ORCID ID: 0000-0002-9277-4972  
[y.zhdanova@kubg.edu.ua](mailto:y.zhdanova@kubg.edu.ua)

**Складаний Павло Миколайович**

старший викладач кафедри інформаційної та кібернетичної безпеки  
Київський університет імені Бориса Грінченка, м. Київ, Україна  
ORCID ID: 0000-0002-7775-6039  
[p.skladannyi@kubg.edu.ua](mailto:p.skladannyi@kubg.edu.ua)

## МІЖДИСЦИПЛІНАРНИЙ ПІДХІД ДО ФОРМУВАННЯ НАВИЧОК УПРАВЛІННЯ РИЗИКАМИ ІБ НА ЗАСАДАХ ТЕОРІЇ ПРИЙНЯТТЯ РІШЕНЬ

**Анотація.** Дана стаття присвячена проблемі готовності студентів спеціальності 125 Кібербезпека у Київському університеті імені Бориса Грінченка до управління ризиками інформаційної безпеки (ІБ) на основі теорії прийняття рішень. Міждисциплінарний підхід до освіти, а саме, інтеграція дисциплін «Теорія ризиків» та «Теорія прийняття рішень», дозволив реалізувати у навчальному процесі формування практичних навичок ризик-менеджменту майбутніх фахівців кібербезпеки. Спираючись на здобутки дидактики та психологічних теорій, здійснено аналіз понять у сфері міждисциплінарної методології та обґрунтовано актуальність і значущість її впровадження у навчальний процес ЗВО. Охарактеризовано особливості організації освітнього процесу підготовки бакалаврів інформаційної та кібернетичної безпеки у контексті міждисциплінарного підходу. Розроблено, теоретично представлено і обґрунтовано елементи методики формування практичних умінь студентів приймати управлінські рішення в умовах ризику на засадах міждисциплінарних принципів. Доведено, що міждисциплінарний обмін, інтеграція теоретичних знань дисциплін сприяють отриманню нових фундаментальних результатів, створюють передумови розвитку практичних навичок, забезпечують цілісний образ підготовки майбутніх фахівців інформаційної та кібернетичної безпеки.

**Ключові слова:** міждисциплінарний підхід; ризики ІБ; управління ризиками ІБ; прийняття рішень; практичні навички студентів; фахівці інформаційної і кібернетичної безпеки.



## ВСТУП

**Постановка проблеми.** Сучасний етап суспільства характеризується впровадженням цифрових технологій у всі сфери людського буття. Разом з цим отримали не лише переваги та покращення життя, але й проблему із захистом інформації як особистої, так і на державному рівні. Кіберзлочинність настільки стала витонченою, що їй важко запобігти. Акцент ставиться тепер на тому, як організація реагує на таке порушення: якщо неможливо його передбачити, то маємо контролювати процес усунення наслідків від порушення, щоб бути готовими і практикуватися в процесі реагування. Розвиток організаційної стійкості дозволить керувати інцидентами, як ще однією частиною бізнесу [1].

Є очевидним, що описані умови вимагають ефективної підготовки фахівців у сфері інформаційної та кібернетичної безпеки. Спеціалісти із захисту інформації мають оволодіти не лише теоретичними знаннями. Вища школа у процесі навчання має закласти підґрунтя для формування та розвитку практичних навичок та умінь управляти системою інформаційної безпеки та оперативно реагувати на порушення конфіденційності, цілісності та доступності інформації.

На значущість досліджуваної проблеми вказують результати наукових психологічних праць [2,3], присвячених питанню «Security-Related Stress» (SRS – стрес, пов'язаний з безпекою). Відсутність досвіду з питань безпеки може спричинити перевантаження, складність та невизначеність. Міжнародні стандарти у сфері захисту інформації розроблені так, щоб бути універсальними, і тим самим надавати можливості для інтерпретації практикуючим. Разом з тим, новачкам потрібно багато часу та зусиль витратити на їх розуміння. У дослідженні [2] констатують, що відсутність у працівників досвіду та знань у галузі безпеки та вимог до безпеки, може призвести до SRS та вплинути на їх рішення у процесі управління інформаційною безпекою.

**Аналіз останніх досліджень і публікацій.** Проведений у рамках дослідження аналіз наукової літератури показав високий інтерес дослідників-науковців до питання професійної підготовки майбутніх фахівців спеціальності 125 Кібербезпека, зокрема, до методологічних аспектів формування практичних навичок студентів. Так, у роботах [4 - 9] представлено результати досліджень і їх впровадження у навчальну діяльність на кафедрі інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка згідно з Освітньою програмою [10] і розробленою моделлю розвитку професійних компетенцій [11].

Зростаюча необхідність вирішення у захисті інформації складних проблем, які виходять за межі можливостей однієї дисципліни, зумовила необхідність впровадження у закладах вищої освіти міждисциплінарний підхід. Міждисциплінарність вирішує існуючі у предметній системі навчання протиріччя між розрізненим засвоєнням знань кожної дисципліни і необхідністю їх синтезу, об'єднання, цілісного та комплексного застосування у практичній діяльності.

Актуальність визначених проблем, їх розв'язання та значущість зумовили дане дослідження.

**Мета статті.** Метою даної статті є розробка елементів методичної системи освітнього процесу підготовки бакалаврів спеціальності 125 Кібербезпека з позицій міждисциплінарного підходу, запровадження якого дозволить більш ефективно формувати їх професійні практичні навички управління ризиками ІБ на засадах теорії прийняття рішень у процесі вивчення дисциплін «Теорія ризиків» та «Теорія прийняття рішень».



## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Аналіз наукових джерел з проблематики дослідження свідчить про те, що ціла низка вітчизняних і зарубіжних дослідників присвятили свої доробки вивченню питань, пов'язаних із міждисциплінарністю [12 - 16], зокрема із міждисциплінарними зв'язками у освітній діяльності фахівців кібербезпеки [17 - 19]. Способи реалізації та наукові положення міждисциплінарного підходу до підготовки фахівців різних спеціальностей висвітлено у працях науковців, серед яких В. Огнев'юк, С. Сисоєва, А. Колот, А. Філіпенко, Т. Коваль, О. Волобуєва та інші. Вони одностайні в тому, що дотримання міждисциплінарних зв'язків є однією з важливих психолого-педагогічних умов підвищення науковості й доступності навчання, його зв'язку із навколишньою дійсністю, активізації підготовчої діяльності й удосконалення процесу формування знань, умінь і навичок у суб'єктів навчання [16].

З'ясуємо сутності та взаємозв'язок понять у сфері міждисциплінарної методології, зокрема поняття «інтеграція» та «міждисциплінарний підхід».

Інтеграція – це об'єднання в ціле будь-яких окремих частин; об'єднання та координація дій різних частин цілісної системи; процес упорядкування, узгодження та об'єднання структур і функцій у цілому організмі; це бік процесу розвитку, що пов'язаний з об'єднанням у ціле раніше різнорідних частин та елементів, а під час процесів інтеграції в уже сформованій системі, або в новій системі, яка виникла з раніше непов'язаних елементів, збільшується обсяг та інтенсивність взаємозв'язків і взаємодій між елементами, зокрема надбудовуються нові рівні управління [20, с. 89].

Виокремлюють різні види інтеграції: тематична інтеграція – здійснення відбору та об'єднання навчального матеріалу з різних предметів з метою цілісного й усебічного вивчення важливих наскрізних тем; повна інтеграція – створення інтегрованих курсів на основі об'єднання в єдине ціле знань з різних предметів [21].

Ми згодні з вченими, які вважають, що принцип міждисциплінарної інтеграції є основним механізмом оптимізації структури моделі знань і системи навчальних дисциплін, який перетворює всю систему підготовки на теоретичний, технологічний і методичний засіб побудови моделей професійної діяльності [16].

Для комплексної характеристики категорії «міждисциплінарність», як стверджує А. Колот, існує необхідність розглядати її як мінімум з дев'яти позицій [13]. Перефразуємо деякі підходи, які є значущими саме для нашого дослідження.

1. Міждисциплінарність – це запозичення і перетікання підходів і методів різних дисциплін.

2. Міждисциплінарність – це здатність побачити, розпізнати, сприйняти те, що стає доступним в межах окремо взятої дисципліни за використання методів та інструментарію інших дисциплін.

3. Міждисциплінарність – це не лише просте запозичення методів, інструментарію з інших дисциплін, а й інтеграція останніх на рівні конструювання міждисциплінарних об'єктів, предметів, опрацювання яких дозволяє отримати нове наукове знання.

4. Міждисциплінарність – це науково-педагогічна новація, що породжує здатність побачити, розпізнати, сприйняти те, що є недоступним в межах окремо взятої дисципліни з її специфічним, вузькоорієнтованим об'єктом, предметом і методами дослідження.

На практиці міждисциплінарний підхід може реалізовуватися за двома основними форматами, сценаріями або підходами [13]. За першого, найбільш поширеного,

міждисциплінарність образно кажучи наводить “мости” між різними дисциплінами, неформально об’єднує їх, не порушуючи їхньої самостійності, унікальності, своєрідності. У даному випадку плюралізм, диференціація дисциплін зберігається, може навіть зростати, а міждисциплінарність надбудовується над ними, пов’язує, об’єднує на методологічному та інструментальному рівні. За другого формату міждисциплінарність постає як реальний інструмент об’єднання дисциплін, появи інтегрованих продуктів, проектів, міждисциплінарних об’єктів дослідження, подальше опанування яких є принципово важливим і для науки, і для освіти.

Важливо усвідомлювати, що міждисциплінарний підхід не поглинає і посягає на метод кожної з наук, а створює передумови для більш рельєфного, широкого погляду на конкретний предмет (об’єкт) дослідження, прирощує наукове знання щодо вирішення поставлених завдань з вищою результативністю [13]

Міждисциплінарний принцип підготовки фахівців є одним з провідних не лише в Україні. На Всесвітній конференції з вищої освіти - 2009: "Нова динаміка вищої освіти і науки для соціальної зміни і розвитку" було наголошено, що системи дослідження потрібно організувати більш гнучко, щоб просувати науку і міждисциплінарність в обслуговуванні суспільства [22].

Для нашого дослідження є важливим вивчити досвід науковців-методистів з даної проблеми саме у підготовці фахівців кібербезпеки. Огляд літератури [17 - 19] дозволив різні моделі і обґрунтування впровадження міждисциплінарного підходу з питань безпеки для школярів, студентів і, навіть, для дорослих для їх неперервної освіти. Так, вчені Johanna Jacob, Michele L. Peters, T. Andrew Yang [17] будують мультидисциплінарну, багаторівневу та багатопотокову модель навчання кібербезпеки на основі мультимодульного підходу. Модель включає питання кримінології, юридичних досліджень та елементів економіки. У дослідженні [18] науковці B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman and R. Leis пропонують пілотну освітню програму прикладно-орієнтовану на людину (нетехнічний аспект). Робота вчених Mat Razali N.A., Ishak K.K., Fadzli M.A.I.M., Saad N.J.A.M [19] висвітлює навчання кібербезпеки з використанням модуля інтегративного навчання (для коледжів, студентів, неперервної освіти дорослих). Дана он-лайн система є міждисциплінарна, на що вказують наступні модулі: «Введення в кібербезпеку», «Етика кібербезпеки», «Програмування та тестування», «Введення в цифрову криміналістику», «Кар’єра в якості експерта з кібербезпеки».

Таким чином, аналіз праць вітчизняних і зарубіжних вчених підтвердив доцільність і актуальність даного дослідження. Міждисциплінарна практика розкриває нові перспективи для своєчасної й адекватної відповіді на актуальні питання безпеки та захисту інформації, для якнайповнішого використання потенціалу дисциплін для досягнення ефекту від їх взаємодії.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

**Постановка проблеми.** Як стверджують зарубіжні експерти, в практиці оцінки ризиків інформаційної безпеки було знайдено багато недоліків, які неминуче ведуть до неправильного прийняття рішень і неадекватним стратегіям безпеки. Тому в даний час все частіше в основу організації процесу управління ІБ закладається більш гнучка, адаптивна стратегія управління ризиками - стратегія ситуаційного управління [1]. Буває контекст надає більше інформації, ніж кількісна оцінка ризиків, і тоді своєчасне

прийняття заходів і засобів протидії загрозам дозволить знизити ризики інформаційної безпеки. На це вказують результати дослідження [23]: чим більше затримка у прийнятті рішень із захисту інформації, тим стрімкіше зростає ризик інформаційної безпеки: так при запізнюванні на 3 години максимальна величина ризику становить 1,57, а вже при запізнюванні на 6 год – 4,93.

Пошук шляхів формування практичних навичок майбутніх фахівців інформаційної і кібернетичної безпеки на основі міждисциплінарного підходу спрямував наші дослідження на розробку елементів методичної системи, модель якої представлено нижче (рис 1).

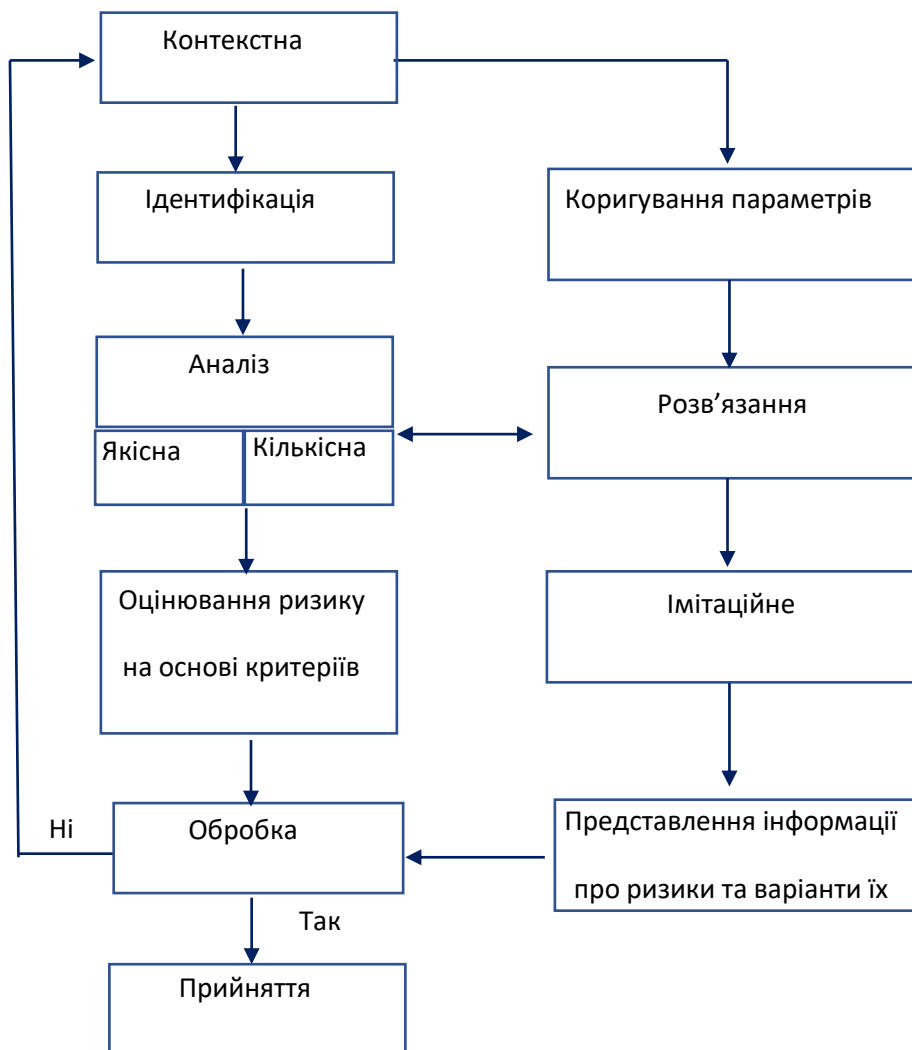


Рисунок 1. Модель взаємодії ризик-менеджменту та прийняття рішень

### 3.2. Змістова складова моделі взаємодії ризик-менеджменту та прийняття рішень

**Крок 1.** Мета навчальної діяльності – удосконалення теоретичних знань та формування практичних навичок управління ризиками інформаційної безпеки (ІБ) за засадах теорії прийняття рішень.



**Крок 2.** Учасники – студенти 3 курсу спеціальності Кібербезпека Київського університету імені Бориса Грінченка.

**Крок 3.** Навчальні дисципліни – Теорія ризиків, Теорія прийняття рішень, Теорія ймовірностей та математична статистика (як допоміжна).

**Крок 4.** Навчальні модулі –

М 1. Ідентифікація, аналіз та оцінка ризиків ІБ.

Поняття ризику ІБ, його сутність та складові. Блок-схема процесу управління ризиком ІБ, основні етапи управління ризиком та їх характеристика. Нормативне забезпечення аналізу та оцінювання ризиків. Міжнародні стандарти забезпечення аналізу та оцінювання ризиків. Методи та засоби якісного та кількісного аналізу та оцінювання ризиків ІБ.

М 2. Обробка ризиків ІБ.

Методи управління ризиками ІБ. Прийоми зниження ризику ІБ. Прийняття ризику ІБ. Моніторинг показників ризиків ІБ.

М 3. Прийняття рішень в управлінні ризиками ІБ.

Правила і критерії прийняття рішень в умовах невизначеності та ризику

**Крок 5.** Форми і методи навчальної діяльності – групова робота у вигляді тренінгу.

**Крок 6.** Формування практичних навичок.

1) Уміння ідентифікувати активи організації, які потрібно захистити та визначити відповідальних за кожний актив.

2) Уміння ідентифікувати уразливості активів.

3) Уміння ідентифікувати загрози.

4) Уміння визначати фактори впливу (уразливості, загрози, наслідки) на величину ризику, якщо загроза реалізується.

5) Уміння визначити рівень ризику по кожній загоді: кількісна оцінка – обчислення ймовірностей; якісна оцінка – проведення SWOT-аналізу та основні експертних оцінок.

6) Уміння здійснювати обробку ризику на основі оптимізаційних задач та імітаційного моделювання

**Крок 7.** Рефлексія.

Сформованість відповідного рівня практичних навичок управління ризиками інформаційної безпеки (ІБ) за засадах теорії прийняття рішень.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Динамічний характер інформаційної та кібернетичної системи захисту вимагає високої фахової компетенції спеціалістів у даній сфері. Аналітичні здібності, уміння працювати єдиною командою, вміння систематизувати інформацію, порівнювати та виявляти спільне та відмінне в даних проблемах, знаходити суперечності і вміти їх розв'язувати, прогнозувати інші шляхи для їх рішення та здійснювати рефлексію цих пошуків – всі ці навички повинні формуватися у навчальному процесі. Вважаємо, що міждисциплінарний підхід в освіті фахівців кібербезпеки забезпечує цілісну картину їх майбутньої діяльності та мотивує на вивчення, сприяє розвитку поліфункціональних професійних навичок.



У перспективі подальших досліджень модель управління ризиками інформаційної безпеки за засадах теорії прийняття рішень буде удосконалена і реалізована у навчальному процесі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1 Malcolm, H. (2016). *Managing Risk and Information Security: Protect to Enable*. <http://Managing-Risk-and-Information-Security.pdf>
- 2 Bergström, E., & Lundgren, M. (2019). Stress Amongst Novice Information Security Risk Management Practitioners. *International Journal on Cyber Situational Awareness*, 4(1), 128–154. <https://doi.org/10.22619/ijcsa.2019.100128>
- 3 D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318. <https://doi.org/10.2753/mis0742-1222310210>
- 4 Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (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), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
- 5 Жданова, Ю., Спасітелева, С., & Шевченко, С. (2019). Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 4(4), 44–53.
- 6 Жданова, Ю., Спасітелева, С., & Шевченко, С. (2019). Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK. *Фізико-математична освіта*, 1(19), 48-54.
- 7 Buriachok, V., Korshun, N., Shevchenko, S., & Skladannyi, P. (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>
- 8 Buriachok, V., Sokolov, V.Y. *Implementation of Active Learning in the Master's Program on Cybersecurity* In: II International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2019), 26-27 January 2019, Kyiv.
- 9 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Skladannyi, P. (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>
- 10 *Освітньо-професійна програма. 125.00.01. Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня освіти*. (2018). Київський університет імені Б. Грінченка. [http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019\\_bak\\_op\\_kiber.pdf](http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf)
- 11 Buriachok, V. L., Bogush, V. M., Borsukovskii, Y. V., Skladannyi, P. M., & Borsukovska, V. Y. (2018). МОДЕЛЬ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ. *Information Technologies and Learning Tools*, 67(5), 277-289. <https://doi.org/10.33407/itlt.v67i5.2347>
- 12 Ognevyuk, V., & Sysoieva, S. (2015). Training of Education Experts in Ukraine: Experimental Interdisciplinary Program. *The Advanced Science Journal*, 2015(6), 98–103. <https://doi.org/10.15550/asj.2015.06.098>
- 13 Колот, А.М. (2014). Міждисциплінарний підхід як домінанта розвитку економічної науки та освітньої діяльності. *Соціальна економік.*, (1-2), 76-83. [http://www.irbis-nbuv.gov.ua/cgi-bin/irbis\\_nbuv/cgiirbis\\_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP\\_meta&C21COM=S&2\\_S21P03=FILE=&2\\_S21STR=se\\_2014\\_1-2\\_15](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILE=&2_S21STR=se_2014_1-2_15)
- 14 Філіпенко, А.С. (2018). Міждисциплінарна методологія: базові принципи, *Міжнародні відносини Серія "Економічні науки" (Спеціальний випуск)*, (13), 7-13. [http://journals.iir.kiev.ua/index.php/ec\\_n/article/viewFile/3283/2959](http://journals.iir.kiev.ua/index.php/ec_n/article/viewFile/3283/2959)
- 15 Коваль, Т.І. (2017). Міждисциплінарний контекст педагогічної підготовки магістра — майбутнього вчителя-філолога в умовах стрімкого розвитку інформаційно-комунікаційних



- технологій, *Педагогічна освіта: Теорія і практика. Психологія. Педагогіка*, (27).  
<https://pedosvita.kubg.edu.ua/index.php/journal/article/view/141>
- 16 Волобуєва, О.Ф. (2015). Міждисциплінарні (міжпредметні) зв'язки під час підготовки майбутнього фахівця: психологічний аспект. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: Психологічні науки*, (1), 26-42.  
[http://nbuv.gov.ua/UJRN/znprapv\\_pn\\_2015\\_1\\_5](http://nbuv.gov.ua/UJRN/znprapv_pn_2015_1_5)
- 17 Jacob, J., Michele, L., Peters, T., Yang, A. Interdisciplinary Cybersecurity: Rethinking. the Approach and the Process. *National Cyber Summit (NCS) Research Track*, (pp.61-74)  
[https://www.researchgate.net/publication/336033638\\_Interdisciplinary\\_Cybersecurity\\_Rethinking\\_the\\_Approach\\_and\\_the\\_Process](https://www.researchgate.net/publication/336033638_Interdisciplinary_Cybersecurity_Rethinking_the_Approach_and_the_Process)
- 18 B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman and R. Leis. (2016). Cyber workforce development using a behavioral cybersecurity paradigm, *2016 International Conference on Cyber Conflict (CyCon U.S.)*, Washington, DC, USA, (pp. 1-6).  
[https://www.researchgate.net/publication/313450400\\_Cyber\\_workforce\\_development\\_using\\_a\\_behavioral\\_cybersecurity\\_paradigm](https://www.researchgate.net/publication/313450400_Cyber_workforce_development_using_a_behavioral_cybersecurity_paradigm)
- 19 Mat Razali N.A., Ishak K.K., Fadzli M.A.I.M., Saad N.J.A.M. (2019) Cyber Security Education Using Integrative Learning Module for an Optimum Learning Experience. In: Badioze Zaman H. et al. (eds) *Advances in Visual Informatics. IVIC 2019. Lecture Notes in Computer Science*, vol 11870. Springer, Cham.  
[https://www.researchgate.net/publication/337187347\\_Cyber\\_Security\\_Education\\_Using\\_Integrative\\_Learning\\_Module\\_for\\_an\\_Optimum\\_Learning\\_Experience](https://www.researchgate.net/publication/337187347_Cyber_Security_Education_Using_Integrative_Learning_Module_for_an_Optimum_Learning_Experience)
- 20 Ковальова, Т. В., Коврига, Л. П. (2002). *Тлумачний словник української мови*. Синтекс.
- 21 Наволокова, Н. П. (2009). *Енциклопедія педагогічних технологій та інновацій*. Основа.
- 22 Всесвітня конференція з вищої освіти - 2009: "Нова динаміка вищої освіти і науки для соціальної зміни і розвитку" ЮНЕСКО, Париж, 5-8 липня 2009 року.  
[https://zakon.rada.gov.ua/laws/show/952\\_011#Text](https://zakon.rada.gov.ua/laws/show/952_011#Text)
- 23 Кононович, В., Кононович, І., Копитін, Ю., Стайкуца, С. (2014). Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки, *Безпека інформації*, 20(1), 83-91.  
[http://nbuv.gov.ua/UJRN/bezin\\_2014\\_20\\_1\\_16](http://nbuv.gov.ua/UJRN/bezin_2014_20_1_16)





**Volodymyr L. Buriachok**

DSc in Technical Sciences, Professor,  
Head of the Department of Information and Cyber Security  
Borys Grinchenko Kyiv University, Kyiv, Ukraine  
ORCID ID: 0000-0002-4055-1494  
*v.buriachok@kubg.edu.ua*

**Svitlana M. Shevchenko**

PhD, Associate Professor,  
Associate Professor of the Department of Information and Cyber Security  
Borys Grinchenko Kyiv University, Kyiv, Ukraine  
ORCID: 0000-0002-9736-8623  
*s.shevchenko@kubg.edu.ua*

**Yuliia D. Zhdanova**

PhD, Associate Professor,  
Associate Professor of the Department of Information and Cyber Security  
Borys Grinchenko Kyiv University, Kyiv, Ukraine  
ORCID: 0000-0002-9277-4972  
*y.zhdanova@kubg.edu.ua*

**Pavlo M. Skladannyi**

Senior Lecturer of the Department of Information and Cyber Security  
Borys Grinchenko Kyiv University, Kyiv, Ukraine  
ORCID: 0000-0002-7775-6039  
*p.skladannyi@kubg.edu.ua*

## **INTERDISCIPLINARY APPROACH TO THE DEVELOPMENT OF INFORMATION SECURITY RISK MANAGEMENT SKILLS ON THE BASIS OF DECISION-MAKING THEORY**

**Abstract.** This article is devoted to the problem of readiness of students majoring in Information Security at Borys Grinchenko Kyiv University to manage information security risks (IS) based on the decision-making theory. The interdisciplinary approach in education, namely, the integration of the disciplines "Risk Theory" and "Decision Theory", allowed to implement in the educational process the formation of practical skills of risk management of future cybersecurity professionals. Based on the achievements of didactics and psychological theories, the analysis of concepts in the field of interdisciplinary methodology is carried out and the relevance and significance of its introduction into the educational process of institution of higher education is substantiated. The peculiarities of the organization of the educational process of training bachelors of information and cyber security in the context of an interdisciplinary approach are described. The elements of the methodology of formation of practical skills of students to make managerial decisions in the conditions of risk on the basis of interdisciplinary principles are developed, theoretically presented and substantiated. It is proved that interdisciplinary exchange, integration of theoretical knowledge of disciplines contribute to new fundamental results, create preconditions for the development of practical skills, provide a holistic image of training future specialists in information and cyber security.

**Keywords:** interdisciplinary approach; IS risks; IS risk management; decision-making; practical skills of students; information and cyber security specialists.



## REFERENCES

- 1 Malcolm, H. (2016). *Managing Risk and Information Security: Protect to Enable*. <http://Managing-Risk-and-Information-Security.pdf>
- 2 Bergström, E., & Lundgren, M. (2019). Stress Amongst Novice Information Security Risk Management Practitioners. *International Journal on Cyber Situational Awareness*, 4 (1), 128-154. <https://doi.org/10.22619/ijcsa.2019.100128>
- 3 D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31 (2), 285-318. <https://doi.org/10.2753/mis0742-1222310210>
- 4 Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (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), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
- 5 Zhdanova, Y., Spasitul'va, S., & Shevchenko, S. (2019). Stagnation of the library of Security.Cryptography classes for practical preparation of specials for cybersecurity. *Cyberbezpeka: education, science, technology*, 4 (4), 44–53.
- 6 Zhdanova, Y., Spasitul'va, S., & Shevchenko, S. (2019). Formation of IT-specialties students' competencies in the field of information retrieval from the registrations of cryptographic services .NET FRAMEWORK. *Physics and mathematics education*, 1 (19), 48-54.
- 7 Buriachok, V., Korshun, N., Shevchenko, S., & Skladannyi, P. (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>
- 8 Buriachok, V., Sokolov, V.Y. Implementation of Active Learning in the Master's Program on Cybersecurity In: II International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2019), 26-27 January 2019, Kyiv.
- 9 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Skladannyi, P. (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>
- 10 Osvitno-professional program. 125.00.01. Security of information and communal systems of the first (bachelor's) level of education. (2018). Kyiv University named after B. Grinchenko. [http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019\\_bak\\_op\\_kiber.pdf](http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf)
- 11 Buriachok, V. L., Bogush, V. M., Borsukovskii, Y. V., Skladannyi, P. M., & Borsukovska, V. Y. (2018). MODEL OF PREPARATION OF FAKHIVTSIV IN THE SPHERE OF INFORMATION AND CYBERNETIC SECURITY IN THE WAYS OF VISCHO OSVITI UKRAINI. *Information Technologies and Learning Tools*, 67 (5), 277-289. <https://doi.org/10.33407/itlt.v67i5.2347>
- 12 Ognevyuk, V., & Sysoieva, S. (2015). Training of Education Experts in Ukraine: Experimental Interdisciplinary Program. *The Advanced Science Journal*, 2015 (6), 98-103. <https://doi.org/10.15550/asj.2015.06.098>
- 13 Kolot, A.M. (2014). Interdisciplinary discipline as a dominant in the development of economic science and educational activity. *Social Economics* ,. (1-2), 76-83. [http://www.irbis-nbuv.gov.ua/cgi-bin/irbis\\_nbuv/cgiirbis\\_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21IID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP\\_meta&C21C2](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21IID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21C2)
- 14 Filipenko, A.S. (2018). Interdisciplinary Methodology: Basic Principles, *International Vidnosini Series "Economic Sciences"* (Special Issue), (13), 7-13. [http://journals.iir.kiev.ua/index.php/ec\\_n/article/viewFile/3283/2959](http://journals.iir.kiev.ua/index.php/ec_n/article/viewFile/3283/2959)
- 15 Koval, T.I. (2017). The interdisciplinary context of the pedagogical training of a master - a mighty teacher-philologist in the minds of a smart development of information and communal technologies, Pedagogical education: theory and practice. *Psychology. Pedagogy*, (27). <https://pedosvita.kubg.edu.ua/index.php/journal/article/view/141>
- 16 Volobueva, O.F. (2015). Interdisciplinary (interdisciplinary) links for the hour of preparation for the future: psychological aspect. *Collection of Science Works of the National Academy of State Border Service of Ukraine. Series: Psychological Sciences*, (1), 26-42. [http://nbuv.gov.ua/UJRN/znpnapv\\_pn\\_2015\\_1\\_5](http://nbuv.gov.ua/UJRN/znpnapv_pn_2015_1_5)



- 17 Jacob, J., Michele, L., Peters, T., Yang, A. Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. National Cyber Summit (NCS) Research Track, (pp.61-74) [https://www.researchgate.net/publication/336033638\\_Interdisciplinary\\_Cybersecurity\\_Rethinking\\_the\\_Approach\\_and\\_the\\_Process](https://www.researchgate.net/publication/336033638_Interdisciplinary_Cybersecurity_Rethinking_the_Approach_and_the_Process)
- 18 B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman and R. Leis. (2016). Cyber workforce development using a behavioral cybersecurity paradigm, 2016 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, (pp. 1-6). [https://www.researchgate.net/publication/313450400\\_Cyber\\_workforce\\_development\\_using\\_a\\_behavioral\\_cybersecurity\\_paradigm](https://www.researchgate.net/publication/313450400_Cyber_workforce_development_using_a_behavioral_cybersecurity_paradigm)
- 19 Mat Razali N.A., Ishak K.K., Fadzli M.A.I.M., Saad N.J.A.M. (2019) Cyber Security Education Using Integrative Learning Mod
- 20 Kovalova, T.V., Kovriga, L.P. (2002). Tlumachny vocabulary of the Ukrainian language. Syntax.
- 21 Navolokova, N.P. (2009). Encyclopedia of pedagogical technologies and innovations. The foundation.
- 22 All-day conference on food education - 2009: "New dynamics of food education and science for social development and development" UNESCO, Paris, 5-8 April 2009 rock. [https://zakon.rada.gov.ua/laws/show/952\\_011#Text](https://zakon.rada.gov.ua/laws/show/952_011#Text)
- 23 Kononovich, V., Kononovich, I., Kopitin, Y., Staykutsa, S. (2014). Injection of the reception of receptions from the source of information to the information security, Bezpeka information, 20 (1), 83-91. [http://nbuv.gov.ua/UJRN/bezin\\_2014\\_20\\_1\\_16](http://nbuv.gov.ua/UJRN/bezin_2014_20_1_16)

