



Силабус освітнього компонента

Програма навчальної дисципліни



Теорія ризиків у кібербезпеці

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація**Освітня програма**

Кібербезпека

Рівень освіти

Перший (бакалаврський)

Семестр

5

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

Викладачі, розробники

**СВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.

Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Теорія ризиків у кібербезпеці" спрямована на те, що студенти одержують теоретичні знання про формування і розвиток теорії і практики аналізу та менеджменту ризиків, понятійного апарату та термінології, щодо ризикоутворюючих факторів, структури та моделей ризиків, практичні навички визначення та виконання завдань щодо своєчасних виявлення, оцінки і аналізу ризиків, в кожному конкретному випадку, вміння виконувати постановку задачі щодо управління ризиками, знання вимог міжнародних і вітчизняних стандартів в цій сфері, знання про математичні методи та засоби, які застосовуються для оцінки та аналізу ризиків і роблять

управління ризиками більш ефективним. Набуті знання та вміння можуть бути використані студентами у майбутній професійній діяльності за фахом.

Мета та цілі дисципліни

Мета навчальної дисципліни полягає у тому, щоб дати уявлення про сутність і зміст поняття „ризик”, типи та моделі ризиків, їх класифікацію, визначальні властивості та шляхи формування, методи аналізу та прогнозування ризиків, а також головні принципи управління ризиками в різних сферах людської діяльності.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

«Комп'ютерні мережі», «Математичний аналіз і теорія ймовірностей», «Інформаційна безпека держави».

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Сутність ризику. Механізми виникнення та розвинення ризиків. Ризики в історичному аспекті та в сучасному світі. Основні характеристики ризиків. Особливості розвитку теорії ризиків в різних сферах. Невизначеність та її особливості. Структура ризиків. Моделі (концепції) ризиків. Проблеми оцінювання ризиків в моделі «невизначеність-ризик».	2
Тема 2. Небезпеки, загрози та вразливості об'єктів ризику, види, характеристики, класифікація. Аналіз ризиків: концепції аналізу, види та задачі, методи аналізу.	2
Тема 3. Методи та особливості оцінювання ризиків. Прогнозування ризиків і втрат від їх реалізації. Особливості експертного аналізу і оцінювання ризиків.	2
Тема 4. Організація управління ризиками, процес управління ризиками. Методи управління ризиками в кібербезпеці. Управління інцидентами безпеки.	2
Тема 5. Особливості прийняття рішень про управління окремими специфічними видами ризиків. Психологічні аспекти прийняття рішень в умовах ризику. Комунікація ризику.	2
Лекція 6. Особливості підприємницьких та економічних ризиків. Індивідуальні ризики: оцінювання ризиків передчасної смерті, прийнятність індивідуального ризику, регулювання індивідуального ризику.	2
Лекція 7. Інформаційні ризики. Методи оцінювання. Вартісно-мотиваційний підхід до аналізу інформаційних ризиків.	2
Лекція 8. Міжнародні стандарти з управління ризиками. Стандарти ISO про принципи аналізу та управління інформаційними ризиками. Національне нормативне забезпечення управління ризиками.	2
Загальна кількість годин	16

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Загальний алгоритм комплексного оцінювання ризиків. Розрахунок та оцінка ризику і середнього ризику. Розрахунок та побудова профілю ризиків.	4	0,1

Аналіз вихідних даних для оцінки ризиків. Методи розрахунку індивідуальних і середніх ризиків. Побудова профілю ризику та його інтерпретація. Використання програмних засобів для моделювання ризиків.

Тема 2. Обґрунтування вибору моделей ризиків для типових ситуацій реалізації загроз.

4

0,1

Порівняльна характеристика основних моделей ризиків. Критерії вибору оптимальної моделі. Приклади застосування моделей у сфері кібербезпеки. Оцінка переваг та недоліків моделей.

Тема 3. Обробка результатів групової експертизи, оцінка рівнів компетентності експертів та якості добору групи експертів.

4

0,1

Методи збору експертних оцінок. Розрахунок коефіцієнтів компетентності експертів. Перевірка узгодженості експертних думок. Формування рекомендацій за результатами експертизи.

Тема 4. Побудова моделі компетентності експерта, обробка результатів групової експертизи із залучення модельних оцінок компетентності експертів.

4

0,1

Структура моделі компетентності експерта. Використання вагових коефіцієнтів у моделі. Методи підвищення достовірності експертних оцінок. Приклад практичного застосування моделі.

Тема 5. Розробка положення про внутрішній контроль та управління ризиками.

4

0,1

Структура внутрішнього положення. Розподіл відповідальності за управління ризиками. Методи моніторингу та звітності. Приклади впровадження внутрішнього контролю.

Тема 6. Оцінка економічних ризиків вибору варіанту системи захисту інформації за умов відомих ймовірностей виникнення загроз та відповідних їм втрат.

4

0,1

Методи оцінки економічної доцільності рішень. Розрахунок очікуваних втрат і витрат. Порівняння альтернативних варіантів систем захисту. Використання сценарного підходу.

Тема 7. Оцінювання ризиків загибелі людини від різних факторів і причин та індивідуальних ризиків загибелі та стати жертвою нещасного випадку жителя певного населеного пункту.

4

0,1

Джерела даних для оцінки індивідуальних ризиків. Розрахунок показників смертності й небезпечності. Моделювання ризиків для окремих категорій населення. Інтерпретація результатів у контексті безпеки.

Тема 8. Розрахунок загального ризику можливої реалізації загрози інформаційним ресурсам, які належать до активів корпоративної інформаційної системи за умов відомої шкоди від порушення конфіденційності ресурсу.

4

0,1

Ідентифікація активів корпоративної системи. Оцінка ймовірності реалізації загроз. Розрахунок шкоди від порушення конфіденційності. Побудова інтегрального показника ризику.

Загальна кількість годин

32

$\sum_{i=1}^n a_i=0,8$

Контрольні роботи

Теорія ризиків у кібербезпеці



Національний технічний університет
«Харківський політехнічний інститут»

Тема 1. Сутність ризику та оцінювання його характеристик.

0,1

Розглядається природа ризику, механізми його виникнення та розвитку, історичні аспекти становлення концепції ризику. Аналізуються основні характеристики ризику, поняття невизначеності, структура та моделі ризику. Особлива увага приділяється проблемам оцінювання ризиків у моделі «невизначеність–ризик» та методам кількісного й якісного аналізу.

Тема 2. Методи управління ризиками та міжнародні стандарти.

0,1

Висвітлюється процес управління ризиками у сфері кібербезпеки, методи мінімізації та прогнозування можливих втрат. Розглядаються підходи до управління інцидентами, особливості прийняття рішень в умовах ризику, психологічні та комунікаційні аспекти. Додатково аналізуються міжнародні стандарти ISO та національні нормативні документи у сфері управління ризиками.

Загалом

$$\sum_{i=1}^m b_i = 0,2$$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення

Кількість годин

Тема 1. Основні підходи до класифікації ризиків у кібербезпеці.

8

Вивчення способів поділу ризиків за критеріями джерел, наслідків та сфери виникнення.

Тема 2. Міжнародні стандарти управління ризиками (ISO/IEC 27005, NIST SP 800-30).

8

Ознайомлення з нормативною базою та кращими практиками управління інформаційними ризиками..

Тема 3. Методи кількісної та якісної оцінки ризиків.

7

Аналіз підходів до вимірювання ризиків, їхніх ймовірностей і наслідків..

Тема 4. Використання дерева відмов та дерева подій у моделюванні ризиків.

7

Побудова логічних моделей причин і сценаріїв розвитку інцидентів.

Тема 5. Метод Монте-Карло як інструмент моделювання невизначеності ризиків.

7

Вивчення статистичного підходу для оцінки можливих сценаріїв розвитку подій.

Тема 6. Використання матриць ризиків у прийнятті управлінських рішень.

7

Розгляд методики побудови й застосування матриць «ймовірність – наслідки».

Тема 7. Ризик-менеджмент у банківській сфері та фінансових установах.

7

Дослідження специфіки оцінки й управління ризиками у фінансовому секторі.

Тема 8. Психологічні аспекти сприйняття ризиків та прийняття рішень.

7

Аналіз впливу когнітивних факторів на поведінку в умовах ризику.

Тема 9. Управління ризиками при впровадженні хмарних технологій.

7

Особливості оцінки загроз і вразливостей у середовищі хмарних сервісів.

Тема 10. Стратегії мінімізації та перенесення ризиків у сфері кібербезпеки. Вивчення методів уникнення, зниження, передачі або прийняття ризиків.	7
Загальна кількість годин	72

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Боровик М. В. Ризик-менеджмент : конспект лекцій / М. В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 65 с. URL: <https://eprints.kname.edu.ua/62534/1/%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%B8%D0%BA%2C%20151%D0%9B%2C%202022%2C%20pdf.pdf>
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега, видання друге, перероблене, доповнене – Одеса: ОНАЗ ім. О.С. Попова, 2020. – 327 с. URL: <https://kr-labs.com.ua/books/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8+%D1%82%D0%B0+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8+%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.PDF>
3. Калініченко З.Д. Ризик-менеджмент: навчальний посібник / Дніпро: ДДУВС, 2021. 224 с. URL: <https://nemk.com.ua/wp-content/uploads/2024/04/%D0%9A%D0%B0%D0%BB%D1%96%D0%BD%D1%96%D1%87%D0%B5%D0%BD%D0%BA%D0%BE-%D0%97.-%D0%94.-%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA-%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82.-%D0%9D%D0%B0%D0%B2%D1%87-%D0%BF%D0%BE%D1%81%D1%96%D0%B1.pdf>
4. Посохов І. М., Управління ризиками у підприємстві: навчальний посібник \ І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 с. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/722daaed-43f3-49f4-aa9b-beb5439cce13/content>
5. Стешенко О. Д. Ризикологія: Навч. посібник. – Харків: УкрДУЗТ, 2019. – 180 с. URL: <http://lib.kart.edu.ua/bitstream/123456789/2224/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf>
6. Шклярчук С. Г. Управління фінансовими ризиками: навч. посіб. / С. Г. Шклярчук. — Київ : ДП «Вид. дім «Персонал», 2019. — 494 с. URL: https://maup.com.ua/assets/files/lib/book/upr_fin_ryzik.pdf
7. Roeser Sabine Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, Springer Science & Business Media, 2012, 1187 p. URL: https://books.google.com.ua/books/about/Handbook_of_Risk_Theory.html?id=PyJ_4KYwxNwC&redir_esc=y

Додаткова література

8. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Є. Архипов, А. В. Скиба // Захист інформації. – 2012. – Т. 15. – № 4. – С. 366–375. URL: <https://ktpu.kpi.ua/wp-content/uploads/2016/02/ITB-2015-s.12-16.pdf>
9. Грайворонський М.В., Новіков О.М. «Безпека інформаційно-комунікаційних систем»-К.: Видавнича група ВНУ.-2009.-608 с. URL: https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
10. Даник Ю.Г., Грищук Р.В. Основи кібербезпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.
11. Даник Ю.Г. Національна безпека: запобігання критичним ситуаціям:/ Ю.Г. Даник, Ю.І. Катков, М.Ф. Пічугін – К. : МО України, Житомир: Рута, 2006. – 388 с.
12. Дубровін В. І. Прийняття рішень у процесі управління ризиками проектів / В. І. Дубровін, В.М. Льовкін. – Запоріжжя : ЗНТУ, 2012. – 196 с. URL: <https://eir.zp.edu.ua/server/api/core/bitstreams/9ff5cbef-ce63-4108-b4bb-bcaa34e12651/content>
13. Качинський А.Б. Безпека, загрози та ризик: наукові концепції та математичні методи.-К.: ІПНБ, НА СБУ.- 2004.-472 с. URL: https://scholar.google.com.ua/citations?view_op=list_works&hl=uk&hl=uk&user=-Jx2gWIAAAAJ
14. Качинський А.Б. Безпека складних систем // А.Б. Качинський. – К.: ТОВ «Юстіон», 2017. – 494 с. URL: https://scholar.google.com.ua/citations?view_op=list_works&hl=uk&hl=uk&user=-Jx2gWIAAAAJ
15. Лисенко І. А. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни “Теорія ризиків” [для студ. денної та заочної форми навч. освітнього ступеню “Бакалавр”, за спеціальністю 125 Кібербезпека] Видання оновлене та доповнене / Уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018.– 32 с. URL: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/a1b319d1-2373-4826-881a-48f18e0eaa89/content>
16. Технічні ризики. Теорія та практикум: [Електронний ресурс]: навч. посібник для студ. / О.М. Терентьєв, С. В. Зайченко, А. Й. Клещов, Н. А. Шевчук / КПІ ім. Ігоря Сікорського. -Електронні тестові дані (1 файл: 5207 КБ). Київ: КПІ ім. Ігоря Сікорського, 2020. – 168 с. URL: https://www.researchgate.net/profile/Anton-Kleshchov/publication/340022921_Tehnicni_riziki_Teoria_ta_praktikum/links/5e7325e34585152cdbcfd7161/Tehnicni-riziki-Teoria-ta-praktikum.pdf
17. Danyk Y., Maliarchuk T., Briggs Ch. Hitting Home: Cyber-Hybrid Warfare in Ukraine and Its Impact on the United States the Georgetown Journal of International Affairs (GJIA), 02.2020, gjia.georgetown.edu. URL: https://www.researchgate.net/profile/Chad-Briggs/publication/320897341_Hybrid_War_High-tech_Information_and_Cyber_Conflicts/links/60751d20299bf1f56d51d1a4/Hybrid-War-High-tech-Information-and-Cyber-Conflicts.pdf
18. Danyk Y., Maliarchuk T., Greg Simons Hybrid war and cyber-attacks: creating legal and operational dilemmas, Global Change, Peace & Security, ISSN: 1478-1158 (Print) 1478-1166 (Online) Journal homepage: <https://www.tandfonline.com/loi/cpar20>, <https://doi.org/10.1080/14781158.2020.1732899>
19. BS 7799-3:2006. Information security management systems. Guidelines for information security risk management. URL: <https://ru.scribd.com/document/291784043/bs-7799-3-2006-open>
20. ISO/IEC 16085:2006. Systems and software engineering – Life cycle processes – Risk management. URL: https://online.budstandart.com.ua/catalog/doc-page?id_doc=71810
21. NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards. URL: <https://www.archives.gov/files/era/recompete/sp800-30.pdf>
22. Information Security Management. Part 2. Specification for Information Security Management systems. British Standard BS 7799, Part 2. 2000. URL: http://www.asq0511.org/Presentations/200405/BS7799_Implementation_ASQ_12May04.pdf

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид

навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i – ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i – ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I , ...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої O з округленням до найближчого цілого числа в більшу сторону.

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.

Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

30.08.2025



Завідувач кафедри

Сергій ЄВСЕЄВ

30.08.2025



Гарант ОП

Сергій ЄВСЕЄВ