



Силабус освітнього компонента Програма навчальної дисципліни



Теорія ризиків у кібербезпеці

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

5

Мова викладання

Українська

Викладачі, розробники



МІЛОВ Олександр Володимирович

oleksandr.milov@khpi.edu.ua

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

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж», «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна «ОВТеорія 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 «ОВТеорія ризиків у кібербезпеці» 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності: практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

ПРН–21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

«Теорія ймовірностей» та «Математична статистика».

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

Теми лекційних занять

Тема 1. Сутність ризику.

Ризики в історичному аспекті та в сучасному світі. Основні характеристики ризиків. Особливості розвитку теорії ризиків в різних сферах.

Тема 2. Механізми виникнення та розвитку ризиків.

Невизначеність та її особливості. Структура ризиків. Моделі (концепції) ризиків. Проблеми оцінювання ризиків в моделі «невизначеність-ризик».

Тема 3. Небезпеки, загрози та вразливості об'єктів ризику, види, характеристики, класифікація.

Аналіз ризиків: концепції аналізу, види та задачі, методи аналізу.

Тема 4. Методи та особливості оцінювання ризиків.

Прогнозування ризиків і втрат від їх реалізації. Особливості експертного аналізу і оцінювання ризиків.

Тема 5. Організація управління ризиками, процес управління ризиками.

Методи управління ризиками в кібербезпеці. Управління інцидентами безпеки.

Тема 6. Особливості прийняття рішень про управління окремими специфічними видами ризиків.

Психологічні аспекти прийняття рішень в умовах ризику. Комунікація ризику.

Лекція 7. Особливості підприємницьких та економічних ризиків.

Індивідуальні ризики: оцінювання ризиків передчасної смерті, прийнятність індивідуального ризику, регулювання індивідуального ризику.

Лекція 8. Інформаційні ризики.

Методи оцінювання. Вартісно-мотиваційний підхід до аналізу інформаційних ризиків.

Лекція 9. Міжнародні стандарти з управління ризиками.

Стандарти ISO про принципи аналізу та управління інформаційними ризиками. Національне нормативне забезпечення управління ризиками.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Загальний алгоритм комплексного оцінювання ризиків.

Тема 2. Розрахунок та оцінка ризику і середнього ризику. Розрахунок та побудова профілю ризиків.

Тема 3. Обґрунтування вибору моделей ризиків для типових ситуацій реалізації загроз

Тема 4. Обробка результатів групової експертизи, оцінка рівнів компетентності експертів та якості добору групи експертів
Тема 5. Побудова моделі компетентності експерта, обробка результатів групової експертизи із залучення модельних оцінок компетентності експертів.
Тема 6. Розробка положення про внутрішній контроль та управління ризиками
Тема 7. Оцінка економічних ризиків вибору варіанту системи захисту інформації за умов відомих ймовірностей виникнення загроз та відповідних ним втрат.
Тема 8. Оцінювання ризиків загибелі людини від різних факторів і причин та індивідуальних ризиків загибелі та стати жертвою нещасного випадку жителя певного населеного пункту
Тема 9. Розрахунок загального ризику можливої реалізації загрози інформаційним ресурсам, які належать до активів корпоративної інформаційної системи за умов відомої шкоди від порушення конфіденційності ресурсу.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

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

Література та навчальні матеріали

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.: Видавнична група ВВВ.-2009.-608 с. URL: https://is.ipt.kpi.ua/pdf/Graivorovskiy_Novikov.pdf

10. Даник Ю.Г., Гришук 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 «Юстюн», 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. Терент'єв, С. В. Зайченко, А. Й. Кleshchov, 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>

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% семестрової оцінки;
- залік: 40% семестрової оцінки

Шкала оцінювання

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

Студент 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

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Андрій ТКАЧОВ