Силабус освітнього компонента
Програма навчальної дисципліни

Технології управління безпекою бізнес-процесів

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Наукова підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна
Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Штучний інтелект і бізнес-аналітика", "Теорія інформації і кодування", "Технологія управління безпекою бізнес-процесів, "Агентне моделювання" та інших у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти досліджують процес моделювання, проектування та впровадження систем безпеки бізнес-процесів, включаючи процес аудиту безпеки. Крім того, студенти знайомляться з сучасними методами та інструментами аналізу ризиків та впровадження систем управління безпекою, що допомагає їм розуміти, як забезпечити ефективну та надійну безпеку бізнес-процесів в організації.

Мета та цілі дисципліни

Формування системного базового уявлення, первинних знань, вміння і навичок студентів з основ технології управління безпекою бізнес-процесів, як одного із напрямків побудови систем безпеки

підприємств та організацій,надання уявлення про моделі бізнес-процесів та методи їх моделювання на засадах процесного підходу.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ1. Здатність 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 інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність 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 інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5. Здатність до дослідження, системного аналізу 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 інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність 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.
КФ8. Здатність 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 інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. 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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та

довідкової літератури та іншої доступної інформації.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Англійська мова в академічних застосунках.

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 проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Теоретичні основи управління бізнес-процесами та їх безпекою. Розглядаються основні поняття управління бізнес-процесами (BPM), принципи їх побудови, ролі учасників, а також концепції забезпечення безпеки у межах бізнес-процесів.	4
Тема 2. Функціональний і процесний підходи до управління безпекою бізнес-процесів. Порівнюються два підходи до організації управління — функціональний і процесний. Аналізується, як процесний підхід дозволяє підвищити ефективність і безпеку бізнес-процесів.	4
Тема 3. Бізнес-процес і його компоненти. Реінжиніринг бізнес-процесів. Вивчається структура бізнес-процесу, основні елементи та етапи його моделювання. Розглядається методологія реінжинірингу (BPR) для оптимізації процесів та підвищення рівня безпеки.	4
Тема 4. Документування бізнес-процесів. Аналізуються методи формалізації та документування бізнес-процесів. Розглядаються стандарти BPMN, IDEF0, EPC, а також роль документації у підтримці безпеки.	4
Тема 5. Вимірювання і аналіз стану протікання бізнес-процесів. Вивчаються методи збору показників ефективності (KPI), моніторинг і аудит процесів. Розглядаються способи оцінки ризиків і виявлення відхилень, що впливають на безпеку.	4
Тема 6. Формування інтегрованих баз даних для опису бізнес-процесів Розглядаються підходи до створення єдиних інформаційних моделей бізнес-	6

процесів, інтеграція даних з різних джерел і забезпечення їхньої цілісності та захищеності.	
Тема 7. Формування і підтримка інформаційних баз даних управління бізнес-процесами. Вивчаються принципи створення, оновлення та супроводу інформаційних баз управління процесами. Розглядаються механізми доступу, резервного копіювання та контролю безпеки даних.	6
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Визначення впливу факторів зовнішнього і внутрішнього середовища на бізнес-процеси суб'єкта господарювання. Досліджуються фактори макро- та мікросередовища, що впливають на ефективність і безпеку бізнес-процесів. Аналізуються ризики, пов'язані з ринковими, організаційними, технічними та інформаційними змінами.	4	0,1
Тема 2. Виконання опису та аналізу предметної області проектованої системи. Проводиться структурований опис предметної області підприємства або організації, визначаються основні об'єкти, зв'язки, інформаційні потоки. Формується основа для подальшого моделювання процесів і побудови інформаційної системи.	3	0,1
Тема 3. Побудова моделі потоків даних предметної області в методології DFD Створюється діаграма потоків даних (DFD) для відображення руху інформації між процесами, зовнішніми сутностями та сховищами даних. Визначається логіка обробки даних у межах бізнес-процесу.	3	0,1
Тема 4. Розробка технічного завдання до інформаційної системи Виконується формування технічного завдання (ТЗ) на створення або вдосконалення інформаційної системи управління бізнес-процесами. Визначаються функціональні вимоги, обмеження, критерії ефективності та вимоги до безпеки.	3	0,1
Тема 5. Структурно-динамічне моделювання. Мережі Петрі Здійснюється моделювання динаміки бізнес-процесів за допомогою мереж Петрі. Вивчаються стани, переходи та події у процесах. Аналізується можливість виявлення "вузьких місць", конфліктів і збоїв у системі.	3	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}5$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Теоретичні засади та організаційні підходи до управління безпекою бізнес-процесів. Розглядаються базові поняття управління бізнес-процесами (BPM), основні підходи — функціональний і процесний, їх відмінності та переваги у контексті забезпечення безпеки. Аналізується структура бізнес-процесів, ролі учасників, взаємодія процесів, а також принципи побудови системи управління безпекою бізнес-процесів.	0,25
Тема 2. Практичні аспекти моделювання, документування та моніторингу бізнес-процесів. Вивчаються практичні методи побудови, документування, вимірювання та аналізу бізнес-процесів. Розглядаються інструменти для створення інтегрованих баз даних і підтримки інформаційних систем управління бізнес-процесами. Особлива увага приділяється питанням інформаційної безпеки, контролю доступу та моніторингу стану процесів.	0,25
Загалом	$\sum_{i=1}^{m} b_i$=0,5

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та екзамену.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Моделювання бізнес-процесів у нотації BPMN. Вивчення основ графічного моделювання бізнес-процесів у BPMN 2.0. Аналіз ключових елементів: події, дії, шлюзи, потоки даних.	8
Тема 2. Управління ризиками бізнес-процесів. Ознайомлення з методами виявлення, оцінки та мінімізації ризиків, що впливають на ефективність і безпеку бізнес-процесів.	8
Тема 3. Використання ERP-систем у забезпеченні безпеки бізнес-процесів. Розгляд можливостей ERP-платформ (SAP, Oracle, Microsoft Dynamics) для управління процесами та контролю доступу до корпоративних даних.	14
Тема 4. Методологія IDEF0 для опису бізнес-процесів. Вивчення основ функціонального моделювання з використанням нотації IDEF0, побудова діаграм функцій і потоків управління.	7
Тема 5. Аудит бізнес-процесів і систем управління. Ознайомлення з методами проведення аудиту бізнес-процесів, визначення критеріїв ефективності та безпеки, підготовка звіту з рекомендаціями.	7
Тема 6. Інформаційна безпека у процесному управлінні. Розгляд підходів до впровадження політик безпеки у бізнес-процеси, контролю прав доступу та захисту інформаційних потоків.	7
Тема 7. Інтелектуальний аналіз процесів (Process Mining). Вивчення технологій аналізу бізнес-процесів на основі даних журналів подій для виявлення відхилень, неефективності та порушень безпеки.	7
Тема 8. Цифрова трансформація бізнес-процесів. Оцінка впливу цифрових технологій (AI, Big Data, IoT) на автоматизацію та	7

підвищення безпеки бізнес-процесів.	
Тема 9. Управління якістю бізнес-процесів (TQM, ISO 9001) Вивчення систем управління якістю як інструменту забезпечення стабільності та безпеки бізнес-процесів підприємства.	7
Тема 10. Використання CASE-засобів для моделювання та аналізу бізнес-процесів Огляд сучасних інструментів (Bizagi, ARIS, Visual Paradigm, Enterprise Architect) для побудови моделей бізнес-процесів і контролю їхньої безпеки.	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 Інформаційна безпека та інформаційні технології. – Х.; ТОВ “ДІСА ПЛЮС”, 2019. - 322 с. http://library.kpi.kharkov.ua/files/new_postupleniya/ibtait.pdf
2. Кібербезпека та інформаційні технології. – Х.; ТОВ “ДІСА ПЛЮС”, 2020. -380 с.
3. Управління бізнес-процесами: Навч. посібник. – Рівне: НУВГП, 2014. – 158 с. https://ep3.nuwm.edu.ua/8812/1/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%20%D1%8F%20%20%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%B0%D0%BC%D0%B8.pdf
4. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

8. Kostina O. M. Diagnostics and management of business processes in the context of enterprise crisis management / Electronic scientific edition “Ekonomika i suspilstvo”.2017. № 10 – С. 287-297.

https://economyandsociety.in.ua/journals/10_ukr/51.pdf
9. Md Imtiaz Mostafiz, Murali Sambasivan, See Kwong Goh, (2019) "Impacts of dynamic managerial capability and international opportunity identification on firm performance", Multinational Business Review,
https://shura.shu.ac.uk/25047/9/Mostafiz-ImpactsDynamicManagerial%28AM%29.pdf
10. Prodius O.I., Naida E.D. Business process reingineering as a modern management concept // Electronic scientific edition "Ekonomika ta suspilstvo" 2019.

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
0,5	0,5		

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:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) 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 О з округленням до найближчого цілого числа в більшу сторону.

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

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** Станіслав МІЛЕВСЬКИЙ