Силабус освітнього компонента
Програма навчальної дисципліни

Безпека безперервності бізнес-процесів

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Спеціальна (фахова) підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

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

МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проєктами» у студентів бакалавріата та магістратури, «Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у аспірантів .

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, вмінь і навичок студентів з основ управління безперервністю 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).
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.
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.
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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
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.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні заняття – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Мережева та хмарна безпека, Безпека Інтернет речей та сервісів.

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 безперервністю бізнес-процесів та їх безпекою. Розглядаються основні поняття, принципи та моделі забезпечення безперервності бізнесу. Аналізуються підходи до управління ризиками, оцінювання вразливостей і планування відновлення діяльності після інцидентів.	5
Тема 2. Функціональний і процесний підходи до управління безпекою процесів підприємства. Вивчаються особливості функціонального та процесного підходів до організації безпеки бізнесу. Розглядаються методи інтеграції безпеки в бізнес-процеси.	5
Тема 3. Методологічні положення виділення та опису бізнес-процесів підприємства. Бізнес-інжиніринг. Описуються методи аналізу, моделювання та документування бізнес-процесів. Розглядається роль бізнес-інжинірингу в підвищенні ефективності та безпеки діяльності підприємства.	5
Тема 4. Регламентація бізнес-процесів. Вивчаються принципи створення нормативних документів, що регламентують виконання бізнес-процесів. Розглядаються стандарти, політики безпеки, посадові інструкції та процедури реагування на інциденти.	5
Тема 5. Діагностика та оптимізація бізнес-процесів. Аналізуються методи оцінювання ефективності бізнес-процесів, виявлення "вузьких місць" і ризиків. Розглядаються підходи до оптимізації процесів для	4

підвищення їх стійкості та безпеки.	
Тема 6. Формування інтегрованих баз даних для опису бізнес-процесів. Вивчаються методи побудови єдиних баз даних для опису, моніторингу та контролю бізнес-процесів. Розглядаються питання узгодженості, доступності та захисту даних.	4
Тема 7. Формування і підтримка інформаційних баз даних управління бізнес-процесами. Описуються принципи побудови систем підтримки управлінських рішень. Розглядаються інформаційні моделі, сховища даних, а також засоби автоматизації контролю безперервності бізнесу.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Методи та технологія стратегічного аналізу бізнес-процесів. Розгляд основних методів стратегічного аналізу, таких як SWOT, PEST та GAP-аналіз, для виявлення слабких місць бізнес-процесів і розробки заходів щодо забезпечення їх безперервності.	5	0,2
Тема 2. Збалансована система показників як метод управління безперервністю бізнес-процесів. Вивчення концепції Balanced Scorecard (BSC) як інструменту моніторингу ефективності процесів і підтримання стабільності бізнесу.	5	0,1
Тема 3. Розробка функціональної моделі опису системи. Створення моделі, що відображає функції, взаємозв'язки та ролі учасників бізнес-процесів, для подальшої автоматизації та контролю.	5	0,1
Тема 4. Розробка моделі потоків даних системи. Побудова діаграм потоків даних (DFD) з метою аналізу обміну інформацією між компонентами системи та виявлення потенційних загроз безпеці.	5	0,1
Тема 5. Розробка технічного завдання до інформаційної системи. Формування вимог до інформаційної системи управління бізнес-процесами, включаючи аспекти безпеки, відмовостійкості та резервування.	4	0,1
Тема 6. Структура та графи мереж Петрі. Ознайомлення з теоретичними основами мереж Петрі, їх елементами, властивостями та можливостями моделювання бізнес-процесів.	4	0,1
Тема 7. Моделювання за допомогою мереж Петрі. Практичне застосування мереж Петрі для опису, аналізу та оптимізації бізнес-процесів, оцінювання ефективності та виявлення ризиків.	4	0,1

Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Теоретичні основи управління безперервністю бізнес-процесів. Вивчення базових принципів, моделей та методів забезпечення стійкої роботи бізнесу в умовах загроз і ризиків.	0,1
Тема 2. Аналіз і оптимізація бізнес-процесів. Практичне застосування інструментів опису, регламентації та вдосконалення бізнес-процесів з урахуванням вимог безпеки та безперервності.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Концепція управління ризиками в бізнес-процесах. Методи ідентифікації, оцінювання та мінімізації ризиків для забезпечення безперервності діяльності.	9
Тема 2. Міжнародні стандарти з управління безперервністю бізнесу (ISO 22301, ISO 27031). Огляд основних вимог і принципів побудови системи управління безперервністю бізнесу.	9
Тема 3. Методологія BCP (Business Continuity Planning) та DRP (Disaster Recovery Planning). Планування дій у разі кризових ситуацій і катастроф.	9
Тема 4. Резервування ресурсів та відновлення бізнес-процесів. Підходи до створення резервних копій, кластеризації систем і швидкого відновлення роботи.	9
Тема 5. Оцінка зрілості процесів управління безпекою бізнесу. Моделі зрілості (CMMI, COBIT) та їх застосування для аналізу ефективності управління.	9
Тема 6. Використання BPM-систем (Business Process Management) у забезпеченні безпеки процесів. Автоматизація моніторингу, контролю та вдосконалення бізнес-процесів.	9
Тема 7. Інформаційна безпека як складова безперервності бізнесу. Зв'язок між кібербезпекою та стабільністю бізнес-операцій.	8
Тема 8. Аналіз зацікавлених сторін у системі управління бізнес-процесами. Визначення ролей, відповідальностей і взаємодії в межах корпоративної структури.	8
Тема 9. Інструменти моделювання бізнес-процесів (ARIS, Bizagi, BPMN). Порівняння функціональних можливостей сучасних засобів моделювання.	8

Тема 10. Цифрова трансформація та її вплив на безперервність бізнесу. Розгляд ризиків і переваг впровадження цифрових технологій у системи управління процесами.	8
Загальна кількість годин	**86**

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%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

1. 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
2. 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

3. 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
0,8	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:

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

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** Ольга КОРОЛЬ