



Силабус освітнього компонента Програма навчальної дисципліни



Новітні технології захисту інформації

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп'ютерних наук та інформаційних
технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Магістр

Тип дисципліни
Профільна, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники



Євсеєв Сергій Петрович

serhii.yevseiev@khpі.edu.ua

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

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Новітні технології захисту інформації" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ). Опанування методів та засобів технічного захисту інформації на ОКІ. Ознайомлення з каналами витоку інформації та підстав їх утворення. Оволодіння навичками роботи із засобами та комплексами виявлення закладних пристроїв несанкціонованого отримання інформації. Оволодіння навичками роботи із засобами та комплексами захисту інформації на ОКІ. Засвоєння порядку проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Оволодіння організаційно-технічними заходами щодо захисту інформації на ОКІ.

Мета та цілі дисципліни

Навчання студентів принципам визначення загальних вимог до кіберзахисту об'єктів критичної інфраструктури, встановлення переліку базових заходів з кіберзахисту, які повинні бути впроваджені на об'єкті критичної інфраструктури, на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, визначення порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК 3. Здатність до безперервного навчання, придбання нових знань і умінь, у тому числі в галузі, відмінній від професійної.

ЗК 4. Здатність виявляти, ставити та вирішувати проблеми у професійній діяльності.

ЗК 5. Здатність генерувати нові ідеї (креативність) і нестандартні підходи до їхньої реалізації, гнучке адаптування до реальних професійних ситуацій, проявляти творчий підхід, ініціативу.

ЗК 6. Здатність критично оцінювати й переосмислювати накопичений досвід (власний і чужий), аналізувати свою професійну і соціальну діяльність.

ЗК 7. Здатність працювати з інформацією: знаходити і використовувати інформацію з різних джерел, потрібну для розв'язання професійних завдань.

ЗК 11. Здатність до соціальної і професійної взаємодії та співпраці у колективі, командної роботи.

СК 1. Здатність формулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, перевіряти коректність постановки, у тому числі в умовах невизначеності.

СК 3. Здатність обирати, розробляти, досліджувати та застосовувати математичні методи для розв'язання практичних задач моделювання, проектування, керування, прогнозування, прийняття рішень.

СК 7. Здатність до пошуку, вивчення та аналізу науково-технічної інформації, вітчизняного і закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження процесів та систем.

СК 13. Здатність до розробки та експлуатації спеціалізованих програмних засобів обробки великих масивів даних на основі інформаційних технологій розподілених і хмарних обчислень.

СК 14. Здатність до використання сучасних інформаційних технологій інтелектуального аналізу даних, прогнозування, прийняття рішень, інформаційного пошуку і видобування знань.

Результати навчання

РН 1. Демонструвати знання і розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці.

РН 2. Уміти формалізувати задачі, сформульовані мовою певної предметної галузі й обирати раціональний метод вирішення; розв'язувати задачі аналітичними або чисельними методами, оцінювати точність і достовірність отриманих результатів та виконувати їхню інтерпретацію.

РН 4. Уміти поєднувати методи математичного і комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.

РН 7. Уміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символічних алгоритмів.

РН 8. Уміти застосовувати у практичній роботі спеціалізовані програмні продукти і програмні системи комп'ютерної математики, аналізу великих даних тощо.

РН 13. Знати і розуміти методи розв'язання математичних задач інтелектуального інформаційного пошуку та видобування знань.

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)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисциплін профільного пакету ВП*.1, а саме, ВП1.1 – «Методи та технології роботи з великими даними», або ВП2.1 – «Аналіз і синтез природньомовної інформації». А також, необхідно мати знання та практичні навички з дисциплін вільного вибору (ДВВ) профільної підготовки, які викладались в першому семестрі.

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. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Тема 2. Фізичний захист об'єктів критичної інфраструктури.

Історія битв. Хакери. Вплив загроз. Сучасний центр моніторингу та управління безпекою (SOC). Захист інфраструктурних комунікацій.

Тема 3. Кіберзахист інфраструктури.

Основні кіберзагрози для критичної інфраструктури. Зловмисники та їхні інструменти.

Тема 4. Управління кризовими ситуаціями та ліквідація наслідків.

Як організувати ефективне управління кризовими ситуаціями в критичній інфраструктурі. Реалізація концепції на прикладі ОБС України. Класифікатор загроз. Удосконалена модель інфраструктури АБС. Концептуальна та синергетична моделі безпеки. Удосконалення моделі оцінювання рівня захищеності. Координація дій різних агентів під час кризової ситуації.

Тема 5. Захист телекомунікаційної інфраструктури.

Як можна захистити телекомунікаційні мережі від кібератак. Сегментація і мікросегментація мережі. Моніторинг і централізоване управління. Next Generation Firewall (NGFW). Unified threat management (UTM). Інспекція зашифрованого трафіку. Захист від витоку конфіденційної інформації. Впровадження рішень двофакторної аутентифікації. Об'єднання локальних мереж і віддалений доступ.

Тема 6. Захист електроенергетичної інфраструктури.

Загрози і вразливості для електроенергетичної інфраструктури. Атаки на інфраструктуру Інтернету речей. Стратегії та технології для захисту електроенергетичної інфраструктури. Виклики, які стоять перед міжнародним співробітництвом у сфері захисту енергетичної інфраструктури.

Тема 7. Захист фінансової інфраструктури.

Основні загрози та ризики для фінансової інфраструктури, інструменти для їх виявлення та оцінки. Методи та технології для захисту фінансових транзакцій та даних в банках та фінансових установах. Стандарти та регуляторні вимоги для забезпечення безпеки фінансової інфраструктури. Сучасні тенденції та інновації в галузі кібербезпеки для захисту фінансових систем та інфраструктури.

Тема 8. Міжнародна співпраця у захисті критичної інфраструктури.

Міжнародні організації та ініціативи для координації заходів з захисту критичної інфраструктури між країнами. Міжнародні договори і механізми співробітництва для забезпечення безпеки критичної інфраструктури. Зелена книга з питань захисту критичної інфраструктури в Україні. Сектори, об'єкти, системи, що можуть бути віднесені до критичної інфраструктури. Основні загрози критичній інфраструктурі. Державна політика захисту критичної інфраструктури. Стратегічні цілі державної політики захисту критичної інфраструктури. Основні принципи формування захисту критичної інфраструктури в Україні. Система захисту критичної інфраструктури в Україні. Розвиток механізмів захисту критичної інфраструктури в Україні.

Тема 9. Умови виникнення терористичної загрози та заходи протидії.

Аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки. Фактори зародження тероризму. Варіанти класифікації тероризму. Типи терористів. Мотиви терористів. Методи підвищення рівня кіберзахисту критичної інформаційної структури.

Тема 10. Інструментальні засоби управління ризиками інформаційної безпеки об'єктів критичної інфраструктури.

Інструментальні засоби управління ризиками інформаційної безпеки/ Моделі оцінки ризиків компанії Digital Securit. Модель аналізу загроз та вразливостей. Принцип роботи алгоритм. Розрахунок ризиків за загрозою інформаційної безпеки. Завдання контрзаходів. Платіжна інфраструктура.

Тема 11. Система управління як об'єкт кібернетичної безпеки.

Аналіз системи управління як об'єкту кібернетичної безпеки. Особливості аналізу. Основи виявлення та пошуку об'єктів з критичною кібернетичною інфраструктурою.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вивчення загальних вимог до кіберзахисту об'єктів критичної інфраструктури.

Тема 2. Критична інфраструктура за регіонами України. Організаційні засади регіону України як складові національної системи захисту критичної інфраструктури.

Тема 3. Складання відомостей про об'єкт критичної інформаційної інфраструктури визначеного регіону України.

Тема 4. Вивчення особливостей національної система захисту критичної інфраструктури.

Тема 5. Вивчення особливостей формування Технічних вимог на створення спеціалізованого програмного забезпечення «Державний реєстр об'єктів критичної інформаційної інфраструктури».

Тема 6. Дослідження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури банків.

Тема 7. Методичні рекомендації щодо розробки поточного та цільового профілю кіберзахисту.

Методичні рекомендації щодо аналізу поточного та цільового профілю кіберзахисту.

Тема 8. Проведення класифікації заходів кіберзахисту об'єктів критичної інфраструктури.

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 та іспиту.

Література та навчальні матеріали

Основна література

1. Закон України «Про критичну інфраструктуру», від 16.11.2021 № 1882-IX.

<https://zakon.rada.gov.ua/laws/show/1882-20#Text>

2. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», від 19 червня 2019 р. № 518.

<https://zakon.rada.gov.ua/laws/show/518-2019-п#Text>

3. Постанова Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури», від 9 жовтня 2020 р. № 943.

<https://zakon.rada.gov.ua/laws/show/943-2020-п#Text>

4. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601.

<https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>

5. Технічні вимоги на створення спеціалізованого програмного забезпечення «Державний реєстр об'єктів критичної інформаційної інфраструктури». Наказ Державної служби спеціального зв'язку та захисту інформації України, 2022, 31 с.
6. Закон України «Про критичну інфраструктуру» (Проект).
<https://www.kmu.gov.ua/bills/proekt-zakonu-pro-kritichnu-infrastrukturu-ta-ii-zakhist>
7. Постанова Правління Національного банку України «Про затвердження Положення про організацію кіберзахисту в банківській системі України» (Проект).
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjbzpqiy8uEAXoVPEDHYS7A0YQFnoECA0QAQ&url=https%3A%2F%2Fbank.gov.ua%2Fadmin_uploads%2Farticle%2Fproekt_2021-11-04.docx%3Fv%3D6&usg=AOvVaw343iqXO03g_Fy_XreHWOyS&opi=89978449
8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
<https://doi.org/10.15587/978-617-7319-31-2>
10. 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.
<http://dx.doi.org/10.15587/978-617-7319-72-5>
11. 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.
<https://doi.org/10.15587/978-617-7319-57-2>

Додаткова література

12. ISO/IEC 27001. «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою».
13. ISO/IEC 27002. «Інформаційні технології. Методи забезпечення безпеки. Практичні правила керування інформаційною безпекою».
14. ISO/IEC 27005. «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки».

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;
- іспит: 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

Дата погодження, підпис
31.08.2023 р.



Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2023 р.



Гарант ОП
Олексій ГАЛУЗА