Силабус освітнього компонента
Програма навчальної дисципліни

Захист об'єктів критичної інфраструктури

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович
serhii.yevseiev@khpi.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

ГАВРИЛОВА Алла Андріївна
alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 30, з них патентів на корисну модель 2, 3 монографії, з яких 1 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з

дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації» у студентів бакалавріата.

Детальніше про викладача на сайті кафедри

ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua
Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ "ХПІ".

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування» , «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Захист об´єктів критичної інфраструктури" 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

КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

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-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Математичні основи криптології, Комплексні системи захисту інформації.

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

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.
Історії 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, 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.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
CyberOps
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література

1. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#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. Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: Наказ Адміністрації Держспецзв'язку від 02.09.2023 №793
https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veresnya-2023-roku-793
6. Про затвердження Положення про організацію кіберзахисту в банківській системі України: Постанова Правління Національного банку України від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
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.
http://monograph.com.ua/pctc/catalog/view/64/52/231-1
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://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Додаткова література

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
13. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
14. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html .

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

28.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП
Роман КОРОЛЬОВ