Силабус освітнього компонента

Програма навчальної дисципліни

Реагування на кіберінциденти

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
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
5

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».
Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Реагування на кіберінциденти" є вибірковою навчальною дисципліною. Дисципліна спрямована на ознайомлення студентів з концепціями та етапами, які необхідно враховувати на етапах планування та реагування на кібер-подію базуючись на моделі реагування на інциденти CREST та фокусуючись на знаннях та ключових навичках, необхідних для ефективного реагування на кіберінциденти.

Мета та цілі дисципліни

Ознайомлення студентів з концепціями та етапами, які необхідно враховувати на етапах планування та реагування на кібер-подію базуючись на моделі реагування на інциденти CREST та

фокусуючись на знаннях та ключових навичках, необхідних для ефективного реагування на кіберінциденти. Після завершення цього курсу студент матиме навички, необхідні для успішного проведення базового розслідування кібербезпеки, яке дотримується формальної методології та забезпечує належний збір та збереження доказів. Студенти також навчаться ефективно обробляти докази за допомогою різних безкоштовних інструментів з відкритим вихідним кодом та використовувати ці результати для розслідування та чіткого опису інциденту.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації;
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

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)

Інформатика, Програмування..

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. Ризик-менеджмент. Основні поняття та визначення у сфері кібербезпеки. Основні поняття. Класифікація ризиків. Ознаки ризиків. Загальна схема процесу управління ризиками. Етапи управління ризиками. Оцінка ризику. Оцінка загроз і уразливостей. Ризики безпеки Microsoft.	2
Тема 2. Прогнозування кіберзагроз. Шкідливе програмне забезпечення. Типові загрози і атаки. Типові мережні атаки – Розвідка, Доступ та Соціальна інженерія. Мережні атаки – Відмова в обслуговуванні, Переповнення буфера та Ухилення. Хто атакує нашу мережу? Інструменти зловмисників.	2
Тема 3. Ідентифікація активів інформаційних систем. Ідентифікація та класифікація активів. Ідентифікація інформаційних ресурсів. Ідентифікація апаратних активів.Ідентифікація програмного забезпечення. Ідентифікація користувачів та ролей. Оцінка важливості активів. Управління життєвим циклом активів. Моніторинг мережі та інструменти моніторингу.	2
Тема 4. Класифікація кіберінцидентів. Ключові критерії для класифікації кіберінцидентів від легких до складних. Вразливості IP. Вразливості TCP та UDP. IP-сервіси. Корпоративні сервіси. Можливі наслідки для організації або системи при кожному рівні класифікації. Класифікатор загроз.	2
Тема 5. Системи виявлення і запобігання: Використання IDS та IPS. Системи виявлення вторгнень. Системи запобігання вторгнень. Способи моніторингу системи. Аналіз методів виявлення вторгнень. Оцінювання сповіщень Security Onion. Відомі системи виявлення та запобігання вторгнень. Порівняльний аналіз сучасних систем виявлення та запобігання вторгнень.	2
Тема 6 Підходи до побудови моделі загроз та порушника.	2

Механізм деструктивного впливу на інформаційну систему. Модель порушника інформаційної безпеки. Розподіл витоків по винуватцеві. Маніпульований інсайдер. Ображені інсайдери. Нелояльні інсайдери. Введені інсайдери. Класифікація інсайдерів по критерію мотивації. Потенціал зловмисників та їх можливості (методика).	
Тема 7. Аналіз логів: збір, агрегація, інтерпретація. Інструменти для збору лог-даних з різних компонентів мережі та систем. Методи для агрегації лог-файлів з різних джерел в одне централізоване сховище. Нормалізація лог-даних для забезпечення стандартного формату та полегшення їхнього подальшого аналізу. Техніки та алгоритми для виявлення аномалій в логах, які можуть свідчити про кіберзагрози чи інші проблеми. Профілювання мережі та сервера. Загальна система оцінки вразливостей (CVSS). Безпечне керування пристроями.	2
Тема 8. Управління інцидентами інформаційної безпеки. Взаємозв'язок понять. Якісна оцінка СМІБ. Зміст процесу управління інцидентами. Причини виникнення інцидентів. Група розслідування інцидентів. Структура команди з розслідування інцидентів інформаційної безпеки. Розробка нормативних документів з управління інцидентами. Виявлення та аналіз інцидентів інформаційної безпеки. Документування інциденту інформаційної безпеки. Протидія поширенню інциденту. Ідентифікація порушника. Зберігання матеріалів. Контрольні листи спостережень.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Встановлення віртуальної машини CyberOps Workstation. Кібербезпека: практичні приклади. Вивчення відомостей про атаку. Візуалізація "чорних" хакерів. Як стати захисником.	6	0,1
Тема 2. Вивчення процесів, потоків, дескрипторів та реєстру Windows. Створення облікових записів користувачів. Використання Windows PowerShell. Диспетчер завдань Windows. Моніторинг системних ресурсів у Windows та керування ними.	6	0,1
Тема 3. Робота з текстовими файлами в CLI. Знайомство із оболонкою Linux. Linux-сервери. Пошук файлів журналів. Навігація у файловій системі Linux та встановлення дозволів.	6	0,1
Тема 4. Створення кодів. Хешування. Шифрування і розшифрування даних за допомогою OpenSSL. Шифрування і дешифрування даних за допомогою хакерських інструментів. Вивчення Telnet і SSH у Wireshark.	6	0,1
Тема 5. Сховища центрів сертифікації. Правила Snort та правила міжмережного екрану. Конвертування даних в універсальний формат. Інтерпретація даних HTTP та DNS для ізоляції нападників.	4	0,1
Тема 6. Ізоляція скомпрометованого хоста за допомогою кортежу із 5-ти елементів. Дослідження зловмисного програмного забезпечення.	4	0,1

Дослідження атаки на хост Windows.		
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i=0,6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Управління ризиками та прогнозування кіберзагроз. Охоплює основні поняття ризик-менеджменту, класифікацію та оцінку ризиків, аналіз загроз і уразливостей. Розглядаються методи прогнозування кіберзагроз, типові атаки та інструменти зловмисників.	0,1
Тема 2. Ідентифікація активів та класифікація кіберінцидентів. Включає ідентифікацію апаратних, програмних та інформаційних активів, управління життєвим циклом активів і моніторинг мережі. Розглядаються ключові критерії класифікації кіберінцидентів та можливі наслідки для організації.	0,15
Тема 3. Системи моніторингу, аналіз логів та управління інцидентами. Включає використання IDS/IPS, підходи до побудови моделі загроз та порушника, збір, агрегацію та інтерпретацію логів. Розглядаються процеси управління інцидентами, розслідування, документування та протидія поширенню кіберінцидентів.	0,15
Загалом	$\sum_{i=1}^{m} b_i=0,4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи кіберзагроз та атак. Види кіберзагроз, типові атаки та їх вплив на інформаційні системи.	8
Тема 2. Ризик-менеджмент у кібербезпеці. Принципи управління ризиками, оцінка загроз і вразливостей.	8
Тема 3. Прогнозування кіберінцидентів. Методи виявлення потенційних загроз і прогнозування атак на інформаційні системи.	7
Тема 4. Ідентифікація та класифікація активів. Визначення та класифікація апаратних, програмних та інформаційних активів.	7
Тема 5. Класифікація кіберінцидентів. Рівні складності інцидентів, ключові критерії та наслідки для організації.	7
Тема 6. Системи виявлення та запобігання вторгнень (IDS/IPS). Принципи роботи, порівняльний аналіз сучасних систем, оцінка сповіщень.	7
Тема 7. Моделі загроз та порушників. Типи зловмисників, інсайдери, їх мотивація та потенціал.	7
Тема 8. Збір та аналіз логів. Методи агрегації, нормалізації, інтерпретації логів для виявлення кіберзагроз.	7

Тема 9. Управління інцидентами інформаційної безпеки. Процес розслідування, документування, контроль і протидія поширенню інцидентів.	7
Тема 10. Інструментальні засоби реагування на кіберінциденти. Програмні та технічні засоби моніторингу, аналізу та реагування на інциденти.	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

1. Онлайн-курс CISCO «CyberOps»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Енсон С. Реагування на комп'ютерні інциденти. Прикладний курс / . Стив Енсон. ДМК Пресс, 2021. - 436 с.
https://www.k0d.cc/storage/books/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%B8%20%D0%B5%D1%91%20%D0%B8%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5/Reagirovanie_na_kompyuternye_intsidenty_Prikladnoy_kurs_2021_Stiv_Enson.pdf
2. Johnson, Leighton. Computer incident response and forensics team management: conducting a successful incident response / Leighton Johnson. Elsevier Inc., 2014. – 349 p.
https://readli.net/computer-incident-response-and-forensics-team-management/
3. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 - 330 p.
https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf
4. 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
5. 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
6. 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

1. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model. URL: https://www.iso.org/search.html?q=15408-1.
2. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.

3. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
4. ISO/IEC 31010:2019 Risk management — Risk assessment techniques
5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
6. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
7. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance
8. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
9. ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security

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
0,6	0,4		

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

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

цілого числа в більшу сторону.

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** Сергій ЄВСЕЄВ