Силабус освітнього компонента

Програма навчальної дисципліни

Управління кіберінцидентами

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
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

КОРОЛЬ Ольга Григорівна

olha.korol@khpi.edu.ua

кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Управління кіберінцидентами" є вибірковою навчальною дисципліною. Необхідність управління захистом інформаційно-комунікаційних мереж виникає в самих різних областях – в сфері зв'язку, військової справі й системах безпеки країни, корпоративних інформаційних системах, системах моніторингу та управління, повсякденній діяльності людини. Для рішення завдань бізнесу слід застосовувати не тільки ефективні та зручні IT засоби, а й приділяти велику увагу побудові контуру безпеки серверних систем. Процес виявлення, аналізу, реагування та покращення наслідків деструктивних подій відомий як управління кіберінцидентами. Метою управління кіберінцидентами є пом'якшення впливу деструктивної події.

Мета та цілі дисципліни

Дисципліна спрямована на засвоєння здобувачами теоретичних основ, формування умінь зі здатність вчасно і ефективно реагувати на кіберзагрози та інциденти.
Предметом дисципліни є комплекс процесів, методів і інструментів, спрямованих на забезпечення готовності організації до кіберзагроз і ефективного реагування на них.
Об'єктом є всі аспекти, що стосуються інформаційних систем, даних та інфраструктури, які можуть бути піддані кіберзагрозам або атакам.

Формат занять

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

Компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
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.

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.
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.
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 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційні системи та інтернет технології, 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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин

Тема 1. Вступ до управління кіберінцидентами. Типи кіберінцидентів. Розглядаються основні поняття, класифікація кіберінцидентів (атаки на мережі, витоки даних, шкідливе ПЗ, фішинг, DDoS). Аналізується важливість управління інцидентами та їх вплив на організаційну безпеку.	2
Тема 2. Процес управління кіберінцидентами. Описуються основні етапи: виявлення, ідентифікація, аналіз, стримування, ліквідація, відновлення та пост-інцидентний розбір. Розглядаються моделі NIST, ISO/IEC 27035.	2
Тема 3. Ролі і обов'язки в команді управління кіберінцидентами. Визначаються ролі CSIRT/CERT, керівника команди, аналітиків, спеціалістів з цифрової криміналістики. Обов'язки, взаємодія із зовнішніми структурами, комунікації під час інциденту.	2
Тема 4. Інструменти та технології для управління кіберінцидентами. Розглядаються SIEM-системи, IDS/IPS, EDR/XDR, системи логування, інструменти цифрової криміналістики, платформи автоматизації реагування (SOAR).	2
Тема 5. Стратегії реагування на кіберінциденти. Методи швидкого реагування, стримування та локалізації інцидентів. Розробка планів реагування, сценарне планування, готовність до інцидентів, комунікація з керівництвом і ЗМІ.	2
Тема 6. Юридичні і регуляторні вимоги. Навчання та підвищення обізнаності. Огляд законодавства: GDPR, NIS2, українське законодавство у сфері КІБЗ. Роль політик, документування інцидентів, аудит. Важливість навчання персоналу та симуляцій.	2
Тема 7. Аналіз інцидентів і вдосконалення процесів. Пост-інцидентний аналіз, визначення причин (root cause analysis), розробка рекомендацій, оновлення політик, впровадження заходів для зниження ризику повторення.	2
Тема 8. Майбутні тенденції в управлінні кіберінцидентами. Аналіз сучасних трендів: використання ШІ у виявленні інцидентів, автоматизовані системи реагування, розвиток кіберзлочинності, нові кіберзагрози для IoT, хмари, критичної інфраструктури.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз і виявлення шкідливого ПЗ. Виконання аналізу підозрілих файлів у безпечному середовищі (sandbox), виявлення ознак шкідливого ПЗ, аналіз поведінки, сигнатур та індикаторів компрометації (IoC).	4	0,1
Тема 2. Виявлення та блокування атак типу "відмова в обслуговуванні" (DoS). Практичне моделювання DoS-атаки, аналіз її впливу на систему та налаштування засобів захисту (фаєрволи, IDS/IPS) для її	4	0,1

блокування.		
Тема 3. Симуляція фішинг-атаки та її реагування. Створення навчальної фішинг-кампанії, аналіз отриманих результатів, визначення ступеня ризиків та формування рекомендацій щодо мінімізації загроз.	3	0,1
Тема 4. Інцидентний аналіз та відновлення системи. Виявлення інциденту, аналіз журналів подій, локалізація та усунення наслідків, відновлення систем до безпечного стану.	3	0,1
Тема 5. Реагування на витік даних. Аналіз ситуацій витоку даних, визначення обсягу скомпрометованої інформації, застосування процедур обмеження шкоди та виконання плану відновлення.	3	0,1
Тема 6. Аналіз мережевого трафіку для виявлення аномалій. Використання інструментів (Wireshark, Zeek тощо) для перегляду та аналізу трафіку, виявлення підозрілих патернів і аномалій.	3	0,1
Тема 7. Розробка та тестування планів реагування на інциденти. Створення IRP (Incident Response Plan), тестування його на практичних кейсах, перевірка ефективності прописаних сценаріїв.	3	0,1
Тема 8. Управління комунікаціями під час кіберінциденту. Моделювання процесу інформування керівництва, клієнтів, партнерів та відповідних органів; створення повідомлень та плану комунікацій.	3	0,1
Тема 9. Оцінка вразливостей системи і виправлення уразливостей. Сканування системи на вразливості, аналіз отриманих результатів, пріоритизація ризиків та впровадження патчів або інших методів виправлення.	3	0,1
Тема 10. Оцінка і вдосконалення політики безпеки. Аналіз існуючої політики безпеки, виявлення недоліків, пропозиція покращень та документальне оновлення політики згідно з сучасними стандартами.	3	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 1$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Процес управління кіберінцидентами та класифікація інцидентів. Студент повинен описати основні типи кіберінцидентів (шкідливе ПЗ, фішинг, DDoS, витік даних тощо), їхні характеристики та етапи життєвого циклу обробки інцидентів. Окрема увага приділяється моделям управління (NIST, ISO 27035), а також методам виявлення, аналізу та документування інцидентів.	0,1
Тема 2. Команда реагування на інциденти, інструменти та стратегія реагування. У роботі необхідно розглянути структуру CSIRT/CERT, ролі та обов'язки членів команди, приклади взаємодії під час інциденту. Також потрібно описати інструменти реагування (SIEM, IDS/IPS, EDR, SOAR) та розробити приклад стратегії реагування на конкретний тип інциденту, включаючи дії до, під час і	0,1

після події.	
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 Стандарти та фреймворки управління інцидентами (NIST, ISO/IEC 27035, SANS). Вивчення міжнародних методологій побудови процесів реагування на інциденти.	8
Тема 2. Threat Intelligence та його роль у виявленні та попередженні інцидентів. Джерела TI, типи даних, платформи обміну (STIX/TAXII).	8
Тема 3. MITRE ATT&CK як інструмент моделювання поведінки зловмисників. Матриця атак, її застосування у SOC та IR.	7
Тема 4. Digital Forensics у контексті управління інцидентами. Методи збору, збереження та аналізу цифрових доказів.	7
Тема 5. Побудова та роль Security Operations Center (SOC). Рівні SOC, інструменти моніторингу, автоматизація.	7
Тема 6. Використання SIEM-систем для виявлення інцидентів. Основні функції, кореляція подій, правила виявлення.	7
Тема 7. Аналіз інсайдерських загроз і моделі поведінки співробітників. Ідентифікація ризиків, методи виявлення та запобігання.	7
Тема 8. Кіберінциденти у хмарному середовищі: особливості та виклики. Використання інструментів CSPM, логування, реагування у хмарі.	7
Тема 9. Використання SOAR-платформ для автоматизації реагування. Приклади сценаріїв автоматичного реагування.	7
Тема 10. Кіберкризи та кризовий менеджмент.. Особливості управління масштабними інцидентами, захист репутації та бізнес-продовжуваність.	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. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. [Електронний ресурс]. – Режим доступу : http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Технології захисту інформації./ С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. [Електронний ресурс]. – Режим доступу : http://kist.ntu.edu.ua/textPhD/tzi.pdf
3. Eric C. Thompson, Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. [Електронний ресурс]. – Режим доступу : https://www.google.com.ua/books/edition/Cybersecurity_Incident_Response/DXhvDwAAQBAJ?hl=ru&gbpv=1&dq=Eric+C.+Thompson,+Cybersecurity+Incident+Response:+How+to+Contain,+Eradicate,+and+Recover+from+Incidents&printsec=frontcover
4. Грайворонський М.В. Безпека інформаційно- комунікаційних систем / М.В. Грайворонський, О.М. Новіков – К.: Видавнича група ВНУ, 2009. – 608 с. [Електронний ресурс]. – Режим доступу : https://ela.kpi.ua/items/eba90ce5-b115-4467-b235-b3b5b6000ae0

Додаткова література

5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. [Електронний ресурс]. – Режим доступу : 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. [Електронний ресурс]. – Режим доступу : 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. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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