Силабус освітнього компонента
Програма навчальної дисципліни

Мережева та хмарна безпека

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
1

Мова викладання
Українська, англійська

Викладачі, розробники

ДЖЕНЮК Наталія Володимирівна

nataliia.dzheniuk@khpi.edu.ua
Доцент кафедри кібербезпеки НТУ "ХПІ" .

Кількість публікацій: понад 31, з них патентів на корисну модель 2, понад 13 наукових праць.
Фахівець з комп'ютерних мереж Cisco, кібербезпеки, інтернету речей, захисту мереж та аналітики вторгнень до мережі. Провідний лектор з дисциплін: «Безпека хмарних технологій».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Мережева та хмарна безпека є основною складовою побудови IT-інфраструктури будь-якої сучасної організації чи виробництва. Зараз великі корпоративні мережі поєднують, як наявні ресурси IT-підрозділу, так й ресурси, що орендуються як хмарні сервіси (Cloud Computing). Тому актуальною стає розширена мережева та хмарна безпека, що поєднує локальні засоби безпеки й відповідні ресурси та системні рішення захисту у хмарі.

Мета та цілі дисципліни

Отримання студентами загальних відомостей про принципи побудови комплексних систем захисту інформації для формування контуру мережевої та хмарної безпеки в інформаційно-комунікаційних системах на основі Інтернет-технологій та застосунків; придбання навичок з

нейтралізації типових мережевих та хмарних загроз, використання протоколів для захисту мереж, захисту від шкідливого програмного забезпечення та мережевого трафіку.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у 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.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
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)

Безпека безперервності бізнес-процесів.

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. Особливості побудови мережевих систем. Розгляд основ архітектури комп'ютерних мереж, рівневої моделі OSI, протоколів передачі даних та принципів побудови безпечної мережевої інфраструктури.	4
Тема 2. Особливості побудови хмарних систем. Аналіз архітектури хмарних обчислень, моделей розгортання (IaaS, PaaS, SaaS) та принципів забезпечення безпеки у хмарних середовищах.	4
Тема 3. Модель мережевих та хмарних загроз. Вивчення класифікації кіберзагроз, типових сценаріїв атак у мережах та хмарах, а також побудова моделей загроз для оцінки ризиків.	4
Тема 4. Засоби збору даних. Ознайомлення з методами моніторингу мережевої активності, інструментами збору телеметрії та журналів подій для виявлення інцидентів безпеки.	4
Тема 5. Засоби інформаційного аналізу у мережах. Розгляд інструментів аналізу трафіку (Wireshark, Snort, Zeek), методів виявлення аномалій та побудови профілів поведінки користувачів.	4
Тема 6. Засоби інформаційного аналізу у хмарах. Вивчення сервісів безпеки хмарних провайдерів, систем логування та моніторингу (Azure Security Center, AWS CloudTrail, Google Security Command Center).	4
Тема 7. Моделі атак на мережі та хмари. Аналіз типових атак — DDoS, MITM, SQL Injection, атак на API та контейнерні сервіси; моделювання ланцюга атак (Kill Chain).	4
Тема 8. Засоби захисту мережевих та хмарних систем. Огляд сучасних засобів захисту — міжмережевих екранів, IDS/IPS, VPN, шифрування, управління ідентичністю та політик безпеки у хмарі.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Дослідження особливостей побудови мережевих систем. Ознайомлення з принципами побудови комп'ютерних мереж, топологіями з'єднань, протоколами передачі даних та способами забезпечення їхньої надійності й безпеки.	4	0,1

Тема 2. Дослідження особливостей побудови хмарних систем. Аналіз архітектури хмарних платформ, типів сервісних моделей (IaaS, PaaS, SaaS) та методів розгортання безпечних хмарних середовищ.	4	0,1
Тема 3. Дослідження моделі мережевих загроз. Вивчення класифікації загроз у мережах, методів моделювання ризиків, аналізу типових сценаріїв атак та їх впливу на мережеву інфраструктуру.	4	0,1
Тема 4. Дослідження засобів збору даних. Практичне ознайомлення з інструментами моніторингу мережевого трафіку, журналів подій та збору інформації для подальшого аналізу інцидентів безпеки.	4	0,1
Тема 5. Дослідження засобів інформаційного аналізу у мережах. Використання програмних засобів для аналізу мережевого трафіку, виявлення вторгнень і дослідження методів виявлення аномальної активності.	4	0,1
Тема 6. Дослідження засобів інформаційного аналізу у хмарах. Аналіз інструментів моніторингу та аудиту хмарних середовищ, дослідження систем журналювання та контролю доступу до даних у хмарі.	4	0,1
Тема 7. Дослідження моделей атак на мережі та хмари. Моделювання та аналіз типових атак (DoS, phishing, SQL Injection, brute force), оцінка їхнього впливу на мережеві та хмарні системи.	4	0,1
Тема 8. Дослідження засобів захисту мережевих та хмарних систем. Практичне ознайомлення з технологіями захисту, такими як брандмауери, IDS/IPS, VPN, системи шифрування та управління ідентичностями користувачів.	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. Аналіз мережевих загроз та методів їх нейтралізації. Оцінка основних видів загроз у комп'ютерних мережах, аналіз вразливостей, методів виявлення атак і практичних підходів до забезпечення мережевої безпеки.	0,1
Тема 2. Захист хмарних середовищ та управління ризиками безпеки. Дослідження типових хмарних загроз, політик безпеки, засобів захисту даних у хмарі, аналіз ефективності моделей безпеки та методів реагування на інциденти.	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. Еволюція мережевих технологій та розвиток хмарних обчислень. Вивчення історії розвитку мережевих технологій, появи хмарних сервісів та їхнього впливу на сучасну інформаційну інфраструктуру.	10
Тема 2. Класифікація мережевих архітектур і протоколів. Ознайомлення з моделями OSI та TCP/IP, принципами маршрутизації, комутації та обміну даними у глобальних мережах.	10
Тема 3. Основи безпеки хмарних сервісів. Самостійне дослідження механізмів захисту у хмарних системах, включно з аутентифікацією, авторизацією та управлінням доступом.	10
Тема 4. Сучасні мережеві вразливості та методи їх виявлення. Вивчення типових вразливостей у мережевих сервісах, інструментів сканування безпеки (Nmap, Nessus) та методів запобігання атакам.	8
Тема 5. Основи криптографічного захисту інформації у мережах. Дослідження принципів шифрування, цифрових сертифікатів, SSL/TLS-протоколів і використання криптографії для захисту передавання даних.	8
Тема 6. Політики безпеки та управління ризиками в хмарних середовищах. Аналіз принципів формування політик безпеки, підходів до оцінки ризиків та методів забезпечення відповідності стандартам (ISO 27001, NIST).	8
Тема 7. Технології віртуалізації та контейнеризації. Вивчення принципів роботи віртуальних машин і контейнерів (Docker, Kubernetes) та аспектів їхньої безпеки.	8
Тема 8. Забезпечення безпеки при використанні мереж Wi-Fi. Ознайомлення з типами атак на бездротові мережі, протоколами захисту (WPA2, WPA3) та практичними заходами безпеки.	8
Тема 9. Інструменти моніторингу та реагування на інциденти. Дослідження систем SIEM, IDS/IPS та засобів моніторингу безпеки для виявлення і реагування на кібератаки.	8
Тема 10. Майбутні тенденції у розвитку мережевої та хмарної безпеки. Аналіз сучасних викликів у сфері кібербезпеки, застосування штучного інтелекту, автоматизації та Zero Trust архітектури.	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

1. Онлайн-курс CISCO «Network Defence, PaloAlto (Cloud Security Fundamentals)»
https://www.netacad.com/catalogs/learn?category=course
https://paloaltonetworksacademy.net/course/index.php.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Безпека хмарного середовища [Електронний ресурс]. – Режим доступу : https://www.netacad.com/ru/courses/cybersecurity/cloud-security.
2. Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/amazon-aws-security/.
3. Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/microsoft-azure-security/.
4. Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/google-cloud-platform-security/.
5. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/.

Додаткова література

1. Cloud Computing Security [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm.
2. Computer Network Security [Електронний ресурс]. – Режим доступу : https://www.javatpoint.com/computer-network-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
0,4	0,2		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 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