Силабус освітнього компонента
Програма навчальної дисципліни

Безпека в інформаційно-комунікаційних системах

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
5

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж». Гарант освітньо-професійної програми «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека в інформаційно-комунікаційних системах" є обов`язковою навчальною дисципліною. Дисципліна спрямована на придбання студентами навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

Мета та цілі дисципліни

Формування теоретичних основ законодавчої бази України та міжнародного суспільства в галузі національної та інформаційної безпеки держави, визначення основних вимог щодо формування підтримки та удосконалення систем управління інформаційної безпеки критичних інформаційно-комунікаційних систем, а також визначення місця і ролі інформаційної безпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. 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.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. 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.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту. Основи математичного моделювання систем безпеки.

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. Кібербезпека; загрози, вразливості та атаки. Типові загрози. Кібератаки та різниця між ними. Атаки на бездротові мережі та мобільні пристрої. Атаки на застосунки. Кібербезпека загрози, вразливості та	2

атаки.	
Тема 2. Захист мереж. Причини провадження мережної безпеки. Вектори мережних атак. Загроза, вразливість та ризик. Еволюція зловмисників. Обмін інформацією про загрози та підвищення рівня обізнаності про кібербезпеку.	2
Тема 3. Атаки на базові функції. IPv4 та IPv6. Заголовки пакетів IPv4 та IPv6. Вразливості IP. Атаки ICMP, за методом підсилення та відбиття, з підміною адрес. Вразливості TCP та UDP.	2
Тема 4. Загрози корпоративній діяльності. Вразливості ARP. Отруєння ARP-кешу. Атаки на основі DNS. Протоколи HTTP і HTTPS. Протидія поширеним мережним атакам.	2
Тема 5. Бездротовий мережевий зв'язок. Порівняння бездротових та дротових локальних мереж. Структура кадра 802.11. Утворення з'єднання між бездротовим клієнтом і точкою доступу. Загрози WLAN. Атаки типу «Відмова в обслуговуванні» (DoS-атаки). Маскування SSID та фільтрація MAC-адрес. Стандартні методи аутентифікації 802.11.	4
Тема 6. Інфраструктура мережевої безпеки. Пристрої безпеки. Опис типів брандмауерів. Пристрої запобігання та виявлення вторгнень. Сервіси безпеки. Контроль трафіку за допомогою списків керування доступом (ACL). Списки керування доступом (ACL): важливі функції. Сервери Syslog.	4
Тема 7. Опреаційна система Windows. Дискова операційна система. Версії Windows. Уразливості операційної системи. Архітектура та робота ОС Windows. Рівень апаратної абстракції. Конфігурація та моніторинг Windows. Безпека Windows.	4
Тема 8. Огляд Linux. Основи Linux. Linux у SOC. Робота в Linux Shell. Сервери та клієнти Linux. Базове адміністрування сервера. Файлова система Linux. Робота із графічним інтерфейсом Linux. Робота на Linux-хості.	4
Тема 9. Захист системи та кінцевої точки. Захист систем та пристроїв. Безпека кінцевих точок. Керування загрозами пристрою. Захист від шкідливих програм. Запобігання вторгнень на основі хоста. Безпека застосунків. Система на основі Sandbox.	4
Тема 10. Принципи, методи та процеси кібербезпеки. Куб кібербезпеки. Захист конфіденційності даних. Стани даних. Проблеми захисту збережених даних. Засоби протидії кіберзлочинності. Апаратні та програмні технології.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Packet Tracer – Дослідження ландшафту загроз. Дослідження вразливостей мережних налаштувань. Дослідження вразливостей зловмисного програмного забезпечення для	4	0,1

фішингу. Дослідження вразливостей бездротової мережі та служби DNS.		
Тема 2. Дослідження DNS-трафіку. Захоплення DNS-трафіку. Дослідження трафіку DNS-запиту. Дослідження трафіку DNS-відповіді.	4	0,1
Тема 3. Створення облікових записів користувачів Створення нового облікового запису локального користувача. Перегляд властивостей облікового запису користувача. Зміна облікових записів локальних користувачів.	4	0,1
Тема 4.Робота з текстовими файлами в CLI. Графічні текстові редактори. Текстові редактори командного рядка. Робота з конфігураційними файлами.	4	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Безпека ОС і кінцевих вузлів. Кібербезпека: загрози, вразливості та атаки.	0,6
Загалом	$\sum_{i=1}^{m} b_i$=0,6

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи безпеки інформаційно-комунікаційних систем. Основні принципи забезпечення безпеки (конфіденційність, цілісність, доступність) в інформаційно-комунікаційних системах. Як класифікуються загрози інформаційній безпеці (технічні, людські, організаційні)?	7
Тема 2. Криптографічні методи захисту. Принципи роботи симетричних алгоритмів шифрування (AES, DES) у захисті даних. Роль асиметричних алгоритмів (RSA, ECC) у забезпеченні безпеки комунікацій.	8
Тема 3. Захист мережевих комунікацій. Основні протоколи безпеки (SSL/TLS, IPsec) та їх застосування в мережах. Як захищаються інформаційно-комунікаційні системи від атак типу "man-in-the-middle"?	8
Тема 4. Виявлення та запобігання вторгненням. Принципи роботи систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS). Які методи аналізу (сигнатурний, аномальний) використовуються для виявлення атак?	7

Тема 5. Захист від технічних каналів витоку інформації. Типи технічних каналів витоку (акустичні, електромагнітні) та методи їх блокування. Принципи роботи шумогенераторів та екранування для захисту інформації.	7
Тема 6. Аутентифікація та контроль доступу. Методи аутентифікації (паролі, біометрія, токени) та їх вразливості. Як моделі RBAC і ABAC застосовуються для управління доступом у системах?	7
Тема 7. Безпека програмного забезпечення. Основні вразливості ПЗ (SQL-ін'єкції, XSS) та методи їх усунення. Принципи безпечної розробки ПЗ (OWASP, SDLC).	7
Тема 8. Захист даних у хмарних системах. Як забезпечується безпека даних у хмарних сервісах (AWS, Azure)? Ризики (витік даних, спільний доступ) та методи їх мінімізації в хмарах.	7
Тема 9. Аудит і моніторинг безпеки. Які стандарти (ISO 27001, NIST) використовуються для аудиту інформаційних систем? Процеси моніторингу безпеки (SIEM) та їх роль у виявленні інцидентів.	7
Тема 10. Соціотехнічні та організаційні аспекти безпеки Як соціальна інженерія (фішинг, pretexting) впливає на безпеку інформаційних систем? Оганізаційні заходи (політики безпеки, навчання) для підвищення безпеки.	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 «Безпека кінцевих вузлів»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. 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.
2. М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев. «Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД.». - 2011.
3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література

1. Хорошко В. А. Методи та засоби захисту інформації. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.
2. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с.
Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.
3. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с.
https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
4. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.
https://f.eruditor.link/file/2593296/

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	0,6		

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

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A

освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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** Роман КОРОЛЬОВ