Силабус освітнього компонента
Програма навчальної дисципліни

Антивірусний захист інформації

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
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
8

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. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

МІЛЕВСЬКА Тетяна Сергіївна

Tetiana.Milevska@cs.khpi.edu.ua
Старший викладач кафедри кібербезпеки НТУ «ХПІ».

Автор понад 80 наукових та навчально-методичних праць. Проводить лабораторні та практичні заняття з дисциплін: «Основи математичного моделювання систем безпеки», «Основи наукових досліджень», «Комп'ютерні системи, мережі та комунікації», «Інформаційна безпека держави» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Антивірусний захист інформації" є обов`язковою навчальною дисципліною. Дисципліна спрямована на підвищення рівня формування у студентів знань та умінь, які створять теоретичний і практичний фундамент, необхідний для аналізу загроз виникаючих при зберіганні, обробленні та передачі інформації у галузі інформаційних технологій.

Мета та цілі дисципліни

Отримання студентами необхідних знань щодо основ теорії захисту інформаційних ресурсів в інформаційних системах з застосуванням сучасних методів та засобів антивірусного захисту інформації.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
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.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.
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

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
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.
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.
РН9. Знати та застосовувати законодавство України 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.
РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
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.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
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 150 год. (5 кредитів ECTS): лекції – 24 год., лабораторні роботи – 36 год., самостійна робота – 90 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Комплексний тренінг.

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 в навчальну дисципліну. Загальні поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Предмет, ціль і задачі курсу. Особливості вивчення дисципліни. Загальні поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Портрет сучасного хакера. Основні поняття та визначення.	3
Тема 2. Загрози і вразливості безпровідних мереж та мобільних пристроїв. Шляхи вирішення проблем захисту інформації в мережах. Можливості троянських програм щодо впливу на мобільні пристрої. Історія розвитку мобільних вірусів. Моделі роботи з платними послугами. Захист Android-пристроїв, iOS-пристроїв. Особливості ОС для мобільних пристроїв. Загрози і вразливості безпровідних мереж. Шляхи вирішення проблем захисту інформації в мережах.	3
Тема 3. Захист від вірусів. Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси. Побудова системи антивірусного захисту корпоративної мережі. Засоби і методи захисту інформації у комп'ютерних системах. Антивірусний захист інформації. Аналіз сучасних антивірусних програм.	3
Тема 4. Проблеми інформаційної безпеки мереж. Введення в мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Забезпечення інформаційної безпеки мереж.	3
Тема 5. Застосування технології міжмережевих екранів при організації антивірусного захисту. Функції міжмережевих екранів (МЕ). Особливості функціонування міжмережевих екранів на різних рівнях моделі OSI. Схеми мережевого захисту на базі міжмережевих екранів.	3
Тема 6. Організація захисту на канальному і сеансовому рівнях. Протоколи формування захищених каналів на канальному рівні. Протоколи формування захищених каналів на сеансовому рівні. Захист безпровідних мереж.	3
Тема 7. Організація захисту на мережевому рівні. Протокол IPsec. Архітектура засобів безпеки IPSec. Захист даних, що передаються за допомогою протоколів AH і ESP. Протокол управління криптоключами IKE. Особливості реалізації засобів IPSec.	3
Тема 8. Інфраструктура захисту на прикладному рівні. Управління ідентифікацією і доступом. Організація захищеного віддаленого доступу. Управління доступом за схемою одноразового входу з авторизацією Single Sign – On (SSO). Протокол Kerberos. Завдання управління системою мережевої безпеки. Архітектура управління засобами мережевої безпеки. Функціонування системи управління засобами безпеки. Аудит і моніторинг антивірусної безпеки.	3
Загальна кількість годин	**24**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів. Аналіз сучасних антивірусних програмних продуктів. Конфігурація міжмережевих екранів. Класифікація шкідливого ПЗ: віруси, черв'яки, трояни, руткіти, spyware. Методи поширення та маскування шкідливих програм. Огляд сучасних антивірусних рішень (Kaspersky, ESET, Symantec, Defender). Порівняння сигнатурного та евристичного аналізу. Практика налаштування міжмережевого екрану (firewall) для захисту мережі.	4	0,1
Тема 2. Шкідливе програмне забезпечення. Використання вразливості "Переповнення буферу". Поняття пам'яті процесу та буфера. Механізм виникнення переповнення буфера. Приклади експлойтів для вразливості. Техніки захисту від переповнення буфера (ASLR, DEP). Практичний експеримент із виявлення уразливості.	4	0,1
Тема 3. Шкідливе програмне забезпечення. Використання вразливості "Помилка на одиницю". Визначення та сутність помилки на одиницю (off-by-one error). Приклади експлуатації помилки в коді. Демонстрація виконання небезпечного коду. Методи запобігання логічним помилкам у програмуванні. Практика пошуку та виправлення помилки в коді.	4	0,1
Тема 4. Налаштування бездротової мережі. Основні параметри Wi-Fi мережі. Конфігурація точки доступу. Методи автентифікації користувачів. Шифрування даних у Wi-Fi мережі. Перевірка працездатності та тестування швидкості мережі.	4	0,1
Тема 5. Налаштування базової WLAN з WLC. Поняття WLAN і контролера бездротових мереж (WLC). Реєстрація точки доступу на WLC. Створення SSID та налаштування базової безпеки. Впровадження VLAN для WLAN. Тестування підключення клієнтів.	4	0,1
Тема 6. Налаштування WPA2 Enterprise WLAN з WLC. Відмінності між WPA2-PSK та WPA2-Enterprise. Налаштування RADIUS-сервера для аутентифікації. Інтеграція WLC із сервером автентифікації. Перевірка доступу користувачів у мережу. Аналіз журналів автентифікації.	4	0,1
Тема 7. Налаштування та перевірка Site-to-Site IPsec VPN. Основи технології IPsec VPN. Вибір протоколів і алгоритмів шифрування. Конфігурація тунелю Site-to-Site VPN. Тестування доступності ресурсів через VPN. Аналіз безпеки тунелю та журналів логів.	4	0,1
Тема 8. WEP/WPA2 PSK/WPA2 RADIUS. Порівняння WEP, WPA2-PSK і WPA2-RADIUS. Визначення вразливостей WEP. Практика налаштування WPA2-PSK. Реалізація WPA2-RADIUS у середовищі лабораторії. Оцінка рівня захищеності різних методів.	4	0,1

Тема 9. Налаштування автентифікації на основі сервера за допомогою TACACS і RADIUS. Основні принципи роботи протоколів TACACS+ і RADIUS. Порівняння можливостей та сфер застосування. Конфігурація сервера TACACS+. Конфігурація сервера RADIUS. Перевірка доступу користувачів і аналіз журналів автентифікації.	4	0,1
Загальна кількість годин	**36**	$\sum_{i=1}^{n} a_i$=0,9

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Класифікація шкідливого програмного забезпечення та методи його виявлення. Типи вірусів і методи поширення. Сучасні антивірусні рішення та їхні функції. Порівняння сигнатурного й евристичного аналізу.	,01
Тема 2. Методи експлуатації програмних вразливостей та засоби їх запобігання. Переповнення буфера як одна з найпоширеніших вразливостей. Помилки програмування та їх наслідки (off-by-one). Захисні технології: ASLR, DEP, кодова обфускація.	0,1
Тема 3. Захист інформації у бездротових та віртуальних приватних мережах (VPN). Основні протоколи захисту Wi-Fi (WEP, WPA2-PSK, WPA2-Enterprise). Налаштування та використання VPN для безпечного з'єднання. Порівняльний аналіз TACACS+ та RADIUS.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,3

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Еволюція комп'ютерних вірусів: від перших шкідливих програм до сучасних кібератак. Перші віруси для ПК (Brain, Michelangelo, CIH). Розвиток мережевих черв'яків (Morris, ILOVEYOU, Code Red). Сучасні загрози: ботнети, криптолокери, APT-атаки. Приклади реальних кібератак останніх років.	15
Тема 2. Методи виявлення та нейтралізації шкідливого ПЗ (сигнатурний, евристичний, поведінковий аналіз). Сигнатурний метод: принцип роботи, переваги й недоліки. Евристичний аналіз: пошук підозрілих патернів. Поведінковий аналіз: моніторинг активності програм. Комбіновані методи в сучасних антивірусах.	15
Тема 3. Антивірусні сканери та системи виявлення вторгнень (IDS/IPS): принципи роботи та застосування. Поняття IDS та IPS, відмінності між ними. Популярні системи: Snort, Suricata, Zeek. Методи детектування: сигнатурний і аномалійний аналіз. Практичне застосування IDS/IPS у корпоративних мережах.	15

Тема 4. Технології шифрування та їх роль у протидії шкідливому ПЗ. Основи симетричного та асиметричного шифрування. Використання криптографії для захисту файлів і комунікацій. Роль шифрування у захисті від перехоплення даних. Приклади використання шифрування в антивірусному захисті.	15
Тема 5. Організаційні заходи протидії вірусним атакам: резервне копіювання, політики безпеки, навчання персоналу. Стратегії резервного копіювання (повне, інкрементальне, диференційне). Розробка політик інформаційної безпеки в організації. Людський фактор: фішинг, соціальна інженерія, небезпека «слабких паролів». Практика навчання співробітників основам кібергігієни.	15
Тема 6. Сучасні тенденції в розвитку антивірусного захисту: штучний інтелект, машинне навчання та хмарні технології. Використання AI для виявлення нових типів шкідливого ПЗ. Machine Learning у поведінковому аналізі. Хмарні антивірусні сервіси: переваги й обмеження. Прогноз майбутніх напрямів у сфері кіберзахисту.	15
Загальна кількість годин	**90**

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

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Дудатьєв А. В., Каплун В. А., Семеренко В. П. Захист програмного забезпечення. Частина 1. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 140 с.
https://pdf.lib.vntu.edu.ua/books/2024/LANZ/Dudatev_2005_140.pdf
2. Каплун В. А. Захист програмного забезпечення. Частина 2 : навчальний посібник. / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця: ВНТУ, 2014.
https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14257/Kaplun-6678619f16033b998a0c233b1e652488.pdf?sequence=1&isAllowed=y
3. Synergy of building cybersecurity systems: monograph / S. Yevseyev, 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
4. 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
5. 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

6. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806). URL: https://zakon.rada.gov.ua/laws/show/z0806-13#Text
7. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf
8. RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 2002г. 129с.
https://www.tech-invite.com/y30/tinv-ietf-rfc-3280.html
9. RFC 3281 An Internet Attribute Certificate Profile for Authorization 2002г. 40с.
https://datatracker.ietf.org/doc/rfc3281/
10. RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols 1999г. 72с.
https://www.rfc-editor.org/rfc/rfc2510
11. RFC 2511 Internet X.509 Certificate Request Message Format 1999г. 25с.
https://www.rfc-editor.org/rfc/rfc2511.html

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
0,7	0,3		

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

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A

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.

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** Сергій ЄВСЕЄВ