Силабус освітнього компонента
Програма навчальної дисципліни

Антивірусний захист інформації

Шифр та назва спеціальності
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Національна безпека у сфері кіберзахисту

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
Детальніше про викладача на сайті кафедри

КОРОЛЬ Ольга Григорівна

olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статтей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. 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 "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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
ФК–2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ФК–4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.
ФК–8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

Результати навчання

ПРН–3. 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.
ПРН–7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
ПРН–8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.
ПРН–9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
ПРН–10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ПРН–12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
ПРН–17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
ПРН–19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати

використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

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

Теми лекційних занять

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.
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.
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.
Тема 4. Проблеми інформаційної безпеки мереж.
Введення в мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Забезпечення інформаційної безпеки мереж.
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.
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.
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.
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.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів. Аналіз сучасних антивірусних програмних продуктів. Конфігурація міжмережевих екранів.
Тема 2. Шкідливе програмне забезпечення. Використання вразливості "Переповнення буферу".
Тема 3. Шкідливе програмне забезпечення. Використання вразливості "Помилка на одиницю".
Тема 4. Налаштування бездротової мережі.
Тема 5. Налаштування базової WLAN з WLC.
Тема 6. Налаштування WPA2 Enterprise WLAN з WLC.
Тема 7. Налаштування та перевірка Site-to-Site IPsec VPN.
Тема 8. WEP/WPA2 PSK/WPA2 RADIUS.
Тема 9. Налаштування автентифікації на основі сервера за допомогою TACACS і RADIUS.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024 — Завідувач кафедри — Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП — Андрій ТКАЧОВ