Силабус освітнього компонента
Програма навчальної дисципліни

Моделі та технології забезпечення безпеки інтелектуальних систем

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Професійна підготока, Вибіркова

Семестр
3

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

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор більше 30 публікацій: з них 3 монографії у співавторстві 1 посібник з грифом. Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Моделі та технології забезпечення безпеки інтелектуальних систем" є вибірковою навчальною дисципліною. Дисципліна спрямована на засвоєння теоретичних основ, формування умінь з організації безпеки інтелектуальних систем та отримання знання технологій побудови систем рівня сучасного центру обробки даних, формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанкціонованому доступу та кіберзагроз.

Мета та цілі дисципліни

Знайомство з новітніми моделями та методами захисту інтелектуального кіберпростору; формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанкціонованому доступу та кіберзагроз.

Формат занять

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

Компетентності

КЗ–2. Здатність проводити дослідження на відповідному рівні.
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.
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.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.

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.
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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Технології 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

Теми лекційних занять

Тема 1. Правові аспекти інформаційної безпеки.
Законодавча та нормативно-правова база України у галузі інформаційної та /або кібербезпеки.
Тема 2. Напрямки забезпечення інформаційної безпеки інтелектуальних систем.

Канали несанкціонованого отримання даних. вимикачі електромагнітних коливань. оптичні вимикачі. Елекричне поле. Способи захисту. Магнітне поле. Способи захисту. Класифікація акустичних каналів витоку інформації. Середовище поширення і спосіб перехвату. Напрямки забезпечення інформаційної безпеки. Завдання служби безпеки. Фізичні засоби захисту. Правовий і технічний захист інформації. Аналіз ризиків.

Тема 3. Методи захисту інформації інтелектуальних систем.

Забезпечення інформаційної безпеки. Організаційні заходи. організаційно-технічні заходи. Характеристика захисних дій. Основні визначення. захист інформації. Моделі секретних систем симетричні криптосистеми. Нелінійні вузли замін симетричних криптоалгоритмів. Блочні алгоритми. Поточні алгоритми. Асиметричні схеми шифрування. Класифікація цифрових підписів.

Тема 4. Основні моделі інформаційної безпеки інтелектуальних систем.

Концептуальна модель. Дискреційне розмеження доступу. Модель адепт-50

Модель дискретного доступу Хартсона. Моделі на основі матриці доступу. Модель Харисона-Руззо-Ульмана Модель take-grant . Модель Белла-Лападули. Моделі безпеки на основі тематичної політики. Формальна специфікація та різновиди рольових моделей. Дискреційна модель Кларка-Вільсона. Теоретико-графові моделі комплексної оцінки захищеності.

Тема 5. Внутрішні та зовнішні загрози. Використання IDS та IPS.

Ключові критерії для класифікації кіберінцидентів від легких до складних. Вразливості IP. Вразливості TCP та UDP. IP-сервіси. Корпоративні сервіси. Можливі наслідки для організації або системи при кожному рівні класифікації. Класифікатор загроз**.** Системи виявлення та запобігання вторгнень. Оцінювання сповіщень Security Onion. Інструменти аналізу. Генерація сповіщень. Структура правил Snort .

Тема 6. Управління кризовими ситуаціями та ліквідація їх наслідків.

Організація ефективного управління кризовими ситуаціями в критичній інфраструктурі. Реалізація концепції на прикладі ОБС України. Класифікатор загроз. Удосконалена модель інфраструктури АБС. Концептуальна та синергетична моделі безпеки. Удосконалення моделі оцінювання рівня захищеності . Координація дій різних агентів під час кризової ситуації.

Тема 7. Підходи до побудови моделі загроз та порушника.

Механізм деструктивного впливу на інформаційну систему. Джерела загроз інформації. Модель порушника інформаційної безпеки . Можливі типи порушників. Основні канали витоку інформації. Тип інсайдера. Класифікації інсайдерів за рівнем ризику. Класифікації зовнішнього порушника за наявними у нього знань про інформаційну систему організації.

Тема 8. Політика системи менеджменту.

Система менеджменту інформаційної безпеки. (Загальна) політика інформаційної безпеки. План забезпечення безперебійної діяльності організації в разі нештатних ситуацій.

Тема 9. Аналіз логів. Збір, агрегація, інтерпретація.

Інструменти для збору лог-даних з різних компонентів мережі та систем. Методи для агрегації лог-файлів з різних джерел в одне централізоване сховище. Нормалізація лог-даних. Техніки та алгоритми для виявлення аномалій в логах. Результати аналізу лог-файлів. Профілювання мережі та сервера. Загальна система оцінки вразливостей (CVSS). Профілювання мережі та сервера. Безпечне керування пристроями.

Тема 10. Управління інцидентами інформаційної безпеки інтелектуальних систем.

Взаємозв'язок понять. Зміст процесу управління інцидентами. Причини виникнення інцидентів. Планування і підготовка. Принципи ефективної політики реагування на інциденти інформаційної безпеки. Ресурси і інструментарій розслідування інцидентів інформаційної безпеки. Превентивні заходи. Виявлення та аналіз інцидентів інформаційної безпеки. Ознаки інциденту. Аналіз інцидентів. Документування інциденту. Пріоритезація інцидентів. Розсилка повідомлень про інцидент. Протидія поширенню інциденту. Збір свідчень інциденту і їх обробка. Ідентифікація порушника. Процедура ліквідації наслідків інциденту. Зберігання матеріалів розслідування інцидентів.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та інформаційних систем.
Тема 2. Інструменти прихованого збору технічної інформації з інформаційної системи або комп'ютерної мережі.
Тема 3. Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування.
Тема 4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA. Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus.
Тема 5. Стеганографічні методи захисту інформації.
Тема 6. Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST.
Тема 7. Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega.
Тема 8. Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng.

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.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
DevNet
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. [Електронний ресурс]. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p. [Електронний ресурс]. – Режим доступу: https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf.
3. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013. [Електронний ресурс]. – Режим доступу: http://repository.hneu.edu.ua/jspui/bitstream/123456789/6813/1/%D0%93%D0%B5%D1%88%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%D1%85%20%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf

4. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с. [Електронний ресурс]. – Режим доступу: https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
5. Енсон С. Реагування на комп'ютерні інциденти. Прикладний курс / . Стив Енсон. ДМК Пресс, 2021. - 436 с. [Електронний ресурс]. – Режим доступу:
6. Johnson, Leighton. Computer incident response and forensics team management: conducting a successful incident response / Leighton Johnson. Elsevier Inc., 2014. – 349 p. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/Computer_Incident_Response_and_Forensics/6lJxGXfLWkYC?hl=ru&gbpv=1&dq=Johnson,+Leighton.+Computer+incident+response+and+forensics+team+management:+conducting+a+successful+incident+response+/+Leighton+Johnson.+Elsevier+Inc.,+2014.+%E2%80%93+349+p.&printsec=frontcover
7. Synergy of building cybersecurity systems: monograph / S. Yevseyev, 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
8. 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
9. 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.

Додаткова література :

10. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model. URL: https://www.iso.org/search.html?q=15408-1.
11. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
12. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
13. ISO/IEC 31010:2019 Risk management — Risk assessment techniques
5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
15. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance
16. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
17. ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% 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 — Станіслав МІЛЕВСЬКИЙ