Силабус освітнього компонента
Програма навчальної дисципліни

Аналіз шкідливих програм

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
Наукова підготовка, Обов'язкова

Семестр
1

Мова викладання
Українська

Викладачі, розробники

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

Дисципліна "Аналіз шкідливих програм" спрямована на поглиблене вивчення методів та технологій виявлення, аналізу та нейтралізації шкідливого програмного забезпечення (ШПЗ). Курс охоплює теоретичні основи кібербезпеки, різновиди шкідливих програм, їх механізми роботи, методи розробки та поширення, а також сучасні підходи до їх аналізу та протидії.

Мета та цілі дисципліни

Надати студентам глибокі знання та практичні навички для ефективного виявлення, аналізу та нейтралізації шкідливих програм. Підготувати фахівців, здатних захищати інформаційні системи від кіберзагроз та забезпечувати їхню безпеку.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
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.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в 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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно 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 та критичної інфраструктури, в інформаційних
системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
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.
КФ10. Здатність провадити науково-педагогічну
діяльність, планувати навчання, контролювати і
супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

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.
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 150 год. (5 кредитів ECTS): лекції – 32 год., практичні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Основи управління в проєктах галузі кібербезпеки та 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.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до кібербезпеки та шкідливих програм. Типи шкідливих програм.
Основні поняття кібербезпеки. Класифікація шкідливих програм. Історія розвитку шкідливого ПЗ. Віруси, трояни, черв'яки. Руткіти, шпигунське ПЗ, рекламне ПЗ. Боти та інші спеціалізовані шкідливі програми.
Тема 2. Поняття та види інформаційних війн.
Що таке інформаційна війна: загальне поняття і роль в сучасних конфліктах. Пропагандистська війна. Психологічна війна. Кібернетична війна. Економічна інформаційна війна. Соціальні медіа як поле битви.
Тема 3. Основні поняття стандартів ISO/IEC 27000: «Інформаційна технологія. Методи забезпечення безпеки».
Вступ до стандартів ISO/IEC 27000. Основні поняття та терміни ISO/IEC 27000. Цілі та принципи інформаційної безпеки. Побудова системи управління інформаційною безпекою (ISMS) за стандартами ISO/IEC 27001. Оцінка ризиків інформаційної безпеки.
Тема 4. Види персональних даних у державі. Принципи захисту персональних даних у державі.
Визначення персональних даних. Класифікація персональних даних. Принципи захисту персональних даних.
Тема 5. Правовий захист персональних даних. Підходи до побудови національних правових систем захисту персональних даних.
Права суб'єктів персональних даних.
Тема 6. Базові поняття криптографічних перетворень.
Вимоги до криптографічних методів захисту інформації. Класифікація методів криптографії.
Тема 7 Симетричні та асиметричні алгоритми шифрування.
Основні принципи шифрування. Визначення асиметричного шифрування. Визначення симетричного шифрування. Порівняння.
Тема 8. Комп'ютерна, цифрова та лінгвістична стеганографія.
Визначення стеганографії. Типові формати даних для стеганографії.
Тема 9. Методи та протоколи ідентифікації й автентифікації.
Вступ до ідентифікації та автентифікації. Традиційні методи автентифікації. Біометрична автентифікація. Двофакторна та багатофакторна автентифікація. Протоколи автентифікації в інформаційних системах.
Тема 10. Парольна автентифікація. Основні підходи до управління доступом.
Використання паролів: переваги та недоліки. Вимоги до безпечних паролів: складність, довжина, частота змін. Основні ризики: атаки методом повного перебору, фішинг, перехоплення паролів..
Тема 11. Управління ключовою інформацією.
Класифікація криптографічних ключів. Генерація. Зберігання. Передача.
Тема 12. Квантова криптографія.
Основні принципи. Протокол квантового розподілу ключів. Безпека квантової криптографії. Практичні реалізації квантової криптографії.
Тема 13. Безпека бездротових систем. Аналіз захищеності ІКС.

Принципи функціонування бездротових мереж. Протоколи безпеки бездротових мереж. Методи захисту бездротових мереж. Загрози та атаки на ІКС.
Тема 14. Модель взаємодії систем OSI. Міжмережеві екрани.
Основні рівні моделі OSI. Принципи роботи. Міжмережеві екрани. Моніторинг та управління.
Тема 15. Побудова систем менеджменту інформаційної безпеки.
Нормативно-правова база. Розробка політики інформаційної безпеки. Оцінка ризиків. Управління інцидентами безпеки. Документування та звітність.
Тема 16. Комплексні системи захисту інформації.
Основні компоненти комплексних систем. Методології та підходи до забезпечення безпеки інформації. Захист від внутрішніх загроз. Системи управління доступом.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розгортання pen-test станції.
Тема 2. складання заяви про захист персональних даних.
Тема 3. Підготовка до роботи Metasploit та postgresql.
Тема 4. Збір інформації за допомогою Metasploit.
Тема 5. Пошук вразливостей за допомогою Metasploit.
Тема 6. Енкодери.
Тема 7. Експлоатація вразливостей.
Тема 8. Пост-експлоатація.

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. Діагностика шкідливого програмного забезпечення: методичні вказівки для підготовки до підсумкового контролю. [Електронний ресурс] / укладач Л. Я. Глинчук; ВНУ ім. Лесі Українки. Електронні текстові данні (1 файл: 232 КБ). Луцьк : ВНУ ім. Лесі Українки, 2023. 74 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22086/1/DSHPZ_metod_rekomend_kontrol.pdf
2. Захист інформації в комп'ютерних системах: Конспект лекцій. Краматорськ, 2020 [Електронний ресурс]. – Режим доступу :. [Електронний ресурс]. – Режим доступу: http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/%D0%97_%D0%9A%D0%A1%20%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86_%D0%B9.pdf
3. Каплун В.А., Майданюк В.П. Захист операційних систем. Навчальний посібник. – Вінниця: ВНТУ, 2006. – 180 с. [Електронний ресурс]. – Режим доступу: https://pz.vntu.edu.ua/media/uploads/metod/bpd/BPD_NP.pdf

4. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
5. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: Навч. посібник. Дніпро: Дніпроп. держ. Унт внутріш. справ, 2020. 144 с. URL: https://duikt.edu.ua/ua/lib/1/category/1195/view/486
6. В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Захист систем електронних комунікацій , Видавництво: КНТЕУ – 2019, Стор.164, ISBN: 978-966-629-970-6. URL: https://knute.edu.ua/file/MjkwMjQ=/b6f7ccc72573e35b6f930d8f11f65c51.pdf
7. Філіп Буайа, Мортен К'ярум, Посібник з європейського права у сфері захисту персональних даних. URL: https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ukr.pdf
8. Гуржій Т. О. Правовий захист персональних даних : монографія / Т. О. Гуржій, А. Л. Петрицький. – Київ : Київ. нац. торг.-екон. ун-т, 2019. – 216 с. URL: https://knute.edu.ua/file/MjIxNw==/b73e21e42607356cffa97508e61515db.pdf
9. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с. URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf
10. Євсєев 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. 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
12. 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
13. 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

14. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. URL: https://eztuir.ztu.edu.ua/jspui/bitstream/123456789/8092/1/%D0%A9%D1%83%D1%80.pdf
15. Гапак О.М., КРИПТОАНАЛІЗ. КРИПТОГРАФІЧНІ ПРОТОКОЛИ. Навчальний посібник. – Ужгород; 2021. – 93 с. [Електронний ресурс]. – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36505/1/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7.%20%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D1%96%20%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8.pdf
16. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/contents/data/standard/08/28/82875.html
17. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html
18. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 50% 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 — Станіслав МІЛЕВСЬКИЙ