



Силабус освітнього компонента

Програма навчальної дисципліни



Організаційне забезпечення захисту інформації

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Кібербезпека

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

7

Мова викладання

Українська

Викладачі, розробники



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 статей 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](#)



ГАВРИЛОВА Алла Андріївна

alla.havrylova@khpi.edu.ua

PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 30, з них патентів на корисну модель 2, 3 монографії, з яких 1 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації» у студентів бакалавріата.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Організаційне забезпечення захисту інформації" є вибірковою навчальною дисципліною. Дисципліна призначена для набуття теоретичних знань з захисту інформації та практичних навичок з організації забезпечення захисту інформації. Студенти вивчають основні напрямки, принципи та умови організаційного захисту; основні підходи, вимоги, методи та засоби.

Мета та цілі дисципліни

Формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розподілу і роботи з кадрами.

Формат занять

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

Компетентності

КЗ-2. Знання та розуміння предметної області та розуміння професії.

КЗ-5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН-1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

РН-2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН-3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН-4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН-5. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН-6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН-7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

РН-8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

- РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
- РН-11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
- РН-12. Розробляти моделі загроз та порушника.
- РН-13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
- РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
- РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
- РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
- РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- РН-19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
- РН-21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- РН-23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- РН-25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
- РН-26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
- РН-27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- РН-29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
- РН-30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
- РН-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

РН-32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

РН-33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

РН-34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.

РН-36. Виявляти небезпечні сигнали технічних засобів.

РН-37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН-40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН-42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

РН-43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

РН-44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

РН-45. Застосовувати рині класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

РН-46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

РН-48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН-49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН-51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

РН-52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

РН-53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН-54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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)

Антивірусний захист інформації, Комплексні системи захисту інформації, знання механізмів роботи з MS Word, MS Excel.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Завдання організаційного забезпечення захисту інформації.

Роль організаційних заходів в створенні надійного механізму захисту інформації. Завдання, які вирішуються на організаційному рівні для забезпечення безпеки функціонування інформації.

Тема 2. Аналіз і оцінка загроз інформаційної безпеки об'єкта.

Класифікація загроз щодо інформаційної безпеки за базовими ознаками. Три основних види загроз.

Тема 3. Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації.

Перелік інформації з обмеженим доступом: державна, комерційна, банківська, професійна, службова таємниці, персональні дані і інтелектуальна власність. Огляд способів несанкціонованого доступу. Умови, що сприяють неправомірному володінню конфіденційною інформацією. Показник критерію ступеня відсутності або наявності завданої об'єкту матеріальної та моральної шкоди. Параметри вартості ризику від настання події.

Тема 4. Служба безпеки об'єкта.

Основні завдання служби безпеки. Принципи системи безпеки підприємства. Функції служби захисту інформації підприємства. Перелік підрозділів служби безпеки об'єкта обробки інформації або підприємства і їх функції.

Тема 5. Підбір, розподіл і робота з кадрами.

Етапи процедури відбору персоналу. Перевірка персоналу на благонадійність. Процес перевірки керівних кадрів. Укладання контрактів та угод про секретності. Особливості звільнення співробітників, які володіють конфіденційною інформацією. Підбір, розподіл і робота з кадрами служби безпеки. Дотримання трудової дисципліни і законності, зміцнення фізичного розвитку, здоров'я, підвищення культури. Соціальний захист персоналу служби безпеки.

Тема 6. Організація і забезпечення режиму таємності.

Особливості режиму секретності. Порядок організації режиму секретності. Закриті роботи режиму секретності. Документи, які регламентують роботу підрозділів із захисту державної таємниці. Права працівників підрозділів із захисту державної таємниці. Основні завдання постійно діючих технічних комісій. Структура і зміст переліку відомостей, що становлять конфіденційну інформацію підприємства. Порядок допуску співробітників до відомостей, що становлять комерційну таємницю. Життєвий цикл документів, які містять комерційну таємницю.

Тема 7. Організація пропускового, внутрішньо об'єктового і протипожежного режиму.

Заходи, які регламентує пропусковий режим. Встановлення відповідальності за забезпечення пропускового режиму і збереження матеріальних цінностей у структурних підрозділах.

Документація з пропускового режиму. Заходи внутрішньо об'єктового режиму. Забезпечення протипожежного режиму.

Тема 8. Захист інформації при аваріях та інших екстремальних ситуаціях.

Особливості інформаційного впливу в екстремальних умовах. Превентивні заходи. Питання, які вирішуються і документуються при складанні попереджувального плану дій. Перелік відомостей плану дій.

Тема 9. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва.

Канали поширення конфіденційної інформації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Шаблони документів.

Тема 2. Створення конструкційної сітки документа складної структури.

Тема 3. Використання колонтитулів під час створення бланків документів.

Тема 4. Використання стилів у електронних документах.

Тема 5. Основи створення документів з обчислюваними реквізитами.

Тема 6. Автоматизація створення та розсилання одностипних документів.

Тема 7. Створення переліків відомостей інформації з обмеженим доступом.

Тема 8. Складання та оформлення організаційно-розпорядчих документів.

Тема 9. Ведення документів, що містять інформацію з грифом. Формування справ.

Тема 10. Відбирання та передавання документів на знищення.

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. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Поточна редакція від 27.07.2023.

URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

2. Про науково-технічну інформацію: Закони України від 25 червня 1993 року № 3322-XII. Поточна редакція від 19.04.2014.

URL: <https://zakon.rada.gov.ua/laws/show/3322-12#Text>

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Поточна редакція від 01.01.2024.

URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

4. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII // ВВР України. Поточна редакція від 01.01.2024.

URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.

5. Про захист персональних даних: Закон України від 09.02.2010 №2297-VI // ВВР України. Поточна редакція від 27.10.2022.

URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

6. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226с. URL: https://moodle.znu.edu.ua/pluginfile.php/1142772/mod_resource/content/1/Zahyst_informacii_ASU.PDF
7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Поточна редакція від 07.09.2022.
URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>
8. 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
9. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/6dbd7fae-06f3-4afd-b2f7-871688668ea0/content>
10. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
URL: <http://kist.ntu.edu.ua/textPhD/tzi.pdf>

Додаткова література

1. Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ. ДУТ-КНУ, 2016. 178 с.
https://duikt.edu.ua/uploads/p_303_92597962.pdf
2. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.
http://nbuv.gov.ua/UJRN/rzod_2015_17_3_8
3. Яремчук Ю. Є. Дослідження характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.
<https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34773/93691.pdf?sequence=2&isAllowed=y>

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

Сергій ЄВСЕЄВ