Силабус освітнього компонента
Програма навчальної дисципліни

Правове регулювання кібербезпеки

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
Спеціальна (фахова), Обов'язкова

Семестр
2

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

Навчальна дисципліна "Правове регулювання кібербезпеки" є нормативною навчальною дисципліною. Вивчення дисципліни спрямовано на формування у студентів умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, правового регулювання стану та принципів забезпечення кібербезпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Мета та цілі дисципліни

Засвоєння студентами послідовного формування знання основних положень теорії та практики застосування норм інформаційного права для забезпечення інформаційної безпеки.

Формат занять

Лекції, практичні заняття, 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.

КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь яких інших проявів недоброчесності.
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 частої 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 ріні 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., практичні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Вступ до спеціальності. Ознайомча практика, Інформаційна безпека держави.

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. Поняття, предмет, метод та місце в системі інформаційного права України.
Поняття інформаційного права як галузі права. Концептуальні підходи до формування змісту інформаційного права. Предмет і методи інформаційного права. Принципи інформаційного права. Джерела інформаційного права.
Тема 2. Інформаційне суспільство: поняття, основні засади розвитку в Україні, взаємозв'язок з інформаційною культурою та інформаційною безпекою.
Інформаційне суспільство та інформаційна цивілізація: поняття, позитивні і негативні сторони. Поняття та сутність інформатизації. Основні засади розвитку інформаційного суспільства в Україні. Інформаційна політика на сучасному етапі. Інформаційна безпека: поняття, види. Поняття інформаційної культури.
Тема 3. Інформаційні правовідносини: поняття, зміст, види.
Поняття інформаційних правовідносин та їхній зміст. Предмет і об’єкти інформаційних правовідносин. Поняття, правові ознаки та види інформації. Правовий статус інформації як об’єкта цивільних прав. Інформація як об’єкт права власності. Зміст суб’єктивного права на інформацію. Суб’єкти інформаційних правовідносин. Класифікація інформаційних правовідносин.
Тема 4. Інформаційна діяльність: поняття, види.
Поняття інформаційної діяльності. Основні напрями та види інформаційної діяльності. Інформаційна діяльність органів державної влади. Висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні.
Тема 5. Правове регулювання діяльності друкованих ЗМІ, інформаційних агентств, видавничої, бібліотечної та архівної справи й державної статистики в Україні.
Друковані ЗМІ (преса) в Україні: правовий статус, державна реєстрація, редакційно-видавнича діяльність, державна підтримка та соціальний захист журналістів. Інформаційні агентства: поняття, особливості створення та реєстрації, створення й поширення їхньої продукції Бібліотечна діяльність в Україні: загальні засади, бібліотечна система, права та обов’язки читачів. Архівна діяльність в Україні: Національний архівний фонд та система архівних установ. Видавнича справа в Україні: організація, суб’єкти, державна реєстрація. Книжкова палата України. Правове регулювання державної статистики в Україні.
Тема 6. Правовий режим інформації з обмеженим доступом.
Поняття та види інформації з обмеженим доступом про особу. Захист персональних даних. Захист конфіденційної інформації, що є власністю держави (службової інформації). Державна таємниця в Україні.
Тема 7. Відповідальність за правопорушення у сфері інформаційних відносин.
Поняття та види правопорушень в інформаційній сфері. Цивільні правопорушення в інформаційній сфері. Дисциплінарна відповідальність у сфері інформаційних правовідносин. Адміністративна відповідальність за правопорушення в інформаційні сфері. Кримінальна відповідальність за злочини в інформаційні сфері. Санкції інформаційного права, що містяться в окремих актах законодавства України.

Теми практичних занять

Тема 1. Поняття, предмет, метод та місце в системі інформаційного права України.
Тема 2. Інформаційне суспільство: поняття, основні засади розвитку в україні, взаємозв'язок з інформаційною культурою та інформаційною безпекою.
Тема 3. Інформаційні правовідносини: поняття, зміст, види.
Тема 4. Інформаційна діяльність: поняття, види.
Тема 5. Правове регулювання діяльності друкованих ЗМІ, інформаційних агентств, видавничої, бібліотечної та архівної справи й державної статистики в Україні.
Тема 6. Правовий режим інформації з обмеженим доступом.
Тема 7. Відповідальність за правопорушення у сфері інформаційних відносин.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

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:
Discovering Entrepreneurship, Engaging Stakeholders for Success
https://www.netacad.com/catalogs/learn?category=course

Література та навчальні матеріали

Основна література

1. Про медіа: Закон України редакція від 01.01.2024 № 2849-IX // ВВР України. https://zakon.rada.gov.ua/laws/show/2849-20#n2349
2. Про державну таємницю: Закон України редакція від 01.01.2024 № 3855-XII // ВВР України. https://zakon.rada.gov.ua/laws/show/3855-12#Text
3. Про банки і банківську діяльність: Закон України редакція від 01.01.2024 № 2121-III // ВВР України. https://zakon.rada.gov.ua/laws/show/2121-14#Text
4. Про захист персональних даних: Закон України редакція від 27.10.2022 №2297–VI // ВВР України. https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. Про оперативно-розшукову діяльність: Закон України редакція від 31.03.2023 № 2135-XII // ВВР України. https://zakon.rada.gov.ua/laws/show/2135-12#Text
6. Цивільний кодекс України: Закон України редакція від 30.01.2024 № 435-IV // ВВР України. https://zakon.rada.gov.ua/laws/show/435-15#Text
7. Про хмарні послуги: Закон України редакція від 27.12.2023 № 2075-IX // ВВР України. https://zakon.rada.gov.ua/laws/main/2075-20#Text
8. Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста: Закон України редакція від 31.03.2021 № 540/97-ВР // ВВР України. https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text
9. Про бібліотеки і бібліотечну справу: Закон України редакція від 01.01.2022 № 32/95-ВР // ВВР України. https://zakon.rada.gov.ua/laws/show/32/95-%D0%B2%D1%80#Text
10. Про видавничу справу: Закон України редакція від 31.12.2023 № 318/97-ВР // ВВР України. https://zakon.rada.gov.ua/laws/show/318/97-%D0%B2%D1%80#Text
11. Про обов'язковий примірник документів: Закон України редакція від 31.03.2023 № 22-23, ст.199 // ВВР України. https://zakon.rada.gov.ua/laws/show/595-14#Text
12. Про національний архівний фонд та архівні установи: Закон України редакція від 02.07.2023 № 3814-XII // ВВР України. https://zakon.rada.gov.ua/laws/show/3814-12#Text
13. Про наукову і науково-технічну діяльність: Закони України редакція від 04.01.2024 № 848-VIII // ВВР України. https://zakon.rada.gov.ua/laws/show/848-19#Text
14. Про доступ до публічної інформації: Закони України редакція від 08.10.2023 № 2939-VI // ВВР України. https://zakon.rada.gov.ua/laws/show/2939-17#Text
15. Про звернення громадян: Закони України редакція від 31.12.2023 № 393/96-ВР // ВВР України. https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text.

Додаткова література

16. 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. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
17. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf
18. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. https://drive.google.com/drive/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
19. 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. https://drive.google.com/drive/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
20. 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. https://drive.google.com/drive/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні заняття: 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