Силабус освітнього компонента
Програма практики

Виробнича практика

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 освітнього компонента
Практична підготовка. Обов'язковий

Семестр
6

Мова викладання
Українська

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

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

Головний зміст виробничої практики полягає у залученні студентів до самостійної проектно-конструкторської роботи, ознайомленні з практикою підприємництва, питаннями реалізації теоретичних та практичних розробок в сфері їх професійної діяльності. Проходження студентами виробничої практики орієнтується на отримання основних результатів проектно-конструкторської роботи. Предметом виробничої практики є поглиблення навичок самостійної теоретичної та практичної роботи, розширення світогляду студентів, дослідження проблем практики та вміння пов'язувати їх з обраним напрямом, визначати структуру та логіку майбутнього дипломного проекту.

Мета та завдання

Забезпечення єдності теоретичного та практичного навчання студентів із питань використання методів аналізу протидії сучасним гібридним атакам, оцінки поточного рівня безпеки та вибору механізмів протидії під час дослідження стану предметної області на базі практики, аналізу інфраструктури мережі, технічних засобів комплексної системи захисту інформації, можливості її удосконалення в умовах дії сучасних загроз.

Формат занять

Самостійна робота, індивідуальне завдання (звіт, щоденник практики), консультації. Підсумковий контроль – залік.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–2. Знання та розуміння предметної області та розуміння професії.
КЗ–3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
КЗ–4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ–5. Здатність до пошуку, оброблення та аналізу інформації.
КЗ–6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ–7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
КФ–1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ– 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ–3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ–4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної 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–6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ–7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ–8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ– 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ–10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ–11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
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 освітнього компонента

Загальний обсяг дисципліни – 180 год. (6 кредитів ECTS): самостійна робота – 180 год.

Тривалість практики

Тривалість практики – 4 тижні.

Передумови освітнього компонента (пререквізити)

Дисципліни загальної та спеціальної підготовки у 1-6 семестрах навчання відповідно до переліку освітніх компонентів.

Особливості освітнього компонента, методи та технології навчання

Виробнича практика проводиться на підприємствах (організаціях, установах) на підставі укладених угод з урегулюванням основних питань організації роботи практикантів. Безпосереднє керівництво практикою здійснює керівник практики від Університету (з числа викладачів випускової кафедри). На початку практики здобувачі вищої освіти повинні отримати інструктаж з охорони праці в галузі, ознайомитися з порядком отримання документації та матеріалів.
Здобувачі вищої освіти під час проходження практик зобов'язані:

- до початку практики одержати в керівника практики від Університету направлення, методичні матеріали (методичні вказівки, програму, щоденник, індивідуальне завдання) та консультації щодо оформлення потрібних документів;
- своєчасно прибути на базу практики;
- щоденно відвідувати базу практики;
- у повному обсязі виконувати всі завдання;
- вивчити й дотримуватися правил охорони праці, техніки безпеки і виробничої санітарії та внутрішнього розпорядку;
- відповідати за виконану роботу та її результати;
- вести щоденник практики;
- своєчасно оформити звітну документацію та скласти залік із практики.

Загальна форма звітності за практику – це подання письмового звіту. Основний документ, що відображає поточну діяльність здобувача вищої освіти, етапи виконання завдань, – це щоденник практики. Цей документ є частиною звіту здобувача вищої освіти. Ведення щоденника є обов'язковим під час проходження виробничої практики. Звіт разом з іншими документами (щоденник практики; характеристика з оцінкою практики від керівником практики на підприємстві) подається до захисту. Звіт охоплює відомості про виконання всіх розділів програми практики та індивідуального завдання, а також розділи з питань охорони праці, висновки і пропозиції, список використаної літератури тощо. Оформлюють звіт відповідно до єдиних вимог щодо оформлення текстових документів. Звіт із практики здобувач вищої освіти захищає (з диференційованою оцінкою) в комісії, до складу якої входять керівники практики (за можливістю, і від баз практик), науково-педагогічні працівники, які викладали спеціальні дисципліни. Склад комісій затверджує завідувач кафедри.

Тематика індивідуального завдання

Тематика визначається з урахуванням місця практики за згодою керівників від навчального закладу та місця проходження практики або представляються основні напрями індивідуального завдання.

Приклади тематики індивідуального завдання:

Тематика 1. Аудит кібербезпеки організації.
Тематика 2. Аналіз вразливостей мережевої інфраструктури.
Тематика 3. Захист веб-додатків.
Тематика 4. Розробка та впровадження системи управління інформаційною безпекою.
Тематика 5. Проведення тестування на проникнення (penetration testing).
Тематика 6. Впровадження систем моніторингу та виявлення загроз.
Тематика 7. Управління доступом та автентифікація користувачів.
Тематика 8. Захист мобільних пристроїв та застосунків.
Тематика 9. Забезпечення безпеки хмарних сервісів.
Тематика 10. Аналіз інцидентів інформаційної безпеки та розробка плану реагування.
Тематика 11. Криптографічний захист інформації.
Тематика 12. Соціальна інженерія та захист від несанкціонованого доступу.
Тематика 13. Розробка політики резервного копіювання та відновлення даних.
Тематика 14. Аналіз безпеки Інтернету речей.
Тематика 15. Розробка системи захисту від внутрішніх загроз.
Тематика 16. Впровадження системи безпеки електронної пошти.
Тематика 17. Захист об'єктів критичної інформаційної інфраструктури.
Тематика 18. Захист персональних даних та відповідність GDPR.

Література та навчальні матеріали

Основна література:

1. ДСТУ 7093:2009 Бібліографічний запис. скорочення слів і словосполук, поданих іноземними європейськими мовами. – Київ : Кн. палата України, 2017. – 17 с.
http://www.ukrbook.net/elektr_publ/spysok_skorochen.pdf

2. ДСТУ 3582:2013 Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – Київ: Мінекономрозвитку України, 2014. – 15 с. http://lib.puet.edu.ua/doc/normativ/DSTU_3582_2013.pdf
3. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП ″УкрНДНЦ″, 2016. – 17 с. http://lib.pnu.edu.ua/files/dstu-8302-2015.pdf
4. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП ″УкрНДНЦ″, 2016. – 31 с. https://science.kname.edu.ua/images/dok/derzhstandart_3008_2015.pdf
5. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП ″УкрНДНЦ″, 2015. – 65 с. https://udhtu.edu.ua/wp-content/uploads/2018/03/DSTY_1_5_2015.pdf
6. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. http://kist.ntu.edu.ua/textPhD/tzi.pdf.
7. СТЗВО-ХПІ-3.01-2021 ССОНП. Текстові документи у сфері навчального процесу. Загальні вимоги до виконання (зі змінами). URL: https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-3.01-2021-SSONP.-Tekstovi-dokumenti-u-sferi-navchalnogo-protsesu.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf

Додаткова література :

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
9. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] / ВР України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0155-17#Text.
10. Словник книгознавчих термінів / уклад.: В. Я. Буран, В. М. Медведєва, Г. І. Ковальчук, М. І. Сенченко. – Київ : Аратта, 2003. – 160 с. http://www.irbis-nbuv.gov.ua/everlib/item/er-0001966

Система оцінювання

Критерії оцінювання успішності здобувача та розподіл балів

Бали нараховуються за наступним співвідношенням:
• виконання та оформлення звіту з практики (70%);
• результат оцінювання у вигляді заліку (30%).

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 доброчесності

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність, в тому числі під час відвідування бази практики. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, керівником практики, 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

		Завідувач кафедри
28.08.2024		Сергій ЄВСЕЄВ
		Гарант ОП
28.08.2024		Сергій ЄВСЕЄВ