



Силабус освітнього компонента Програма практики



Технологічна практика

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

-

Освітня програма

Кібербезпека

Рівень освіти

Перший (бакалаврський)

Семестр

8

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Кафедра

Кібербезпеки (328)

Тип освітнього компонента

Практична, Обов'язкова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

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, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)

**ГАВРИЛОВА Алла Андріївна**

alla.havrylova@khpi.edu.ua

PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – 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», «Безпека в DevOps», «Організація та безпека баз даних», «Управління IT-проектами та їх безпека» у студентів бакалавріату.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

При проходженні даного виду практики у здобувачів формуються кваліфікаційні та професійні компетентності на основі синтезу теорії та практики, й проявляється через актуалізацію здатності особистості не тільки розв'язувати фахові задачі, а й висувати й вирішувати професійні проблеми

Мета та завдання

закріплення та поглиблення теоретичних знань із застосування вивчених концепцій (криптографія, мережева безпека, аналіз вразливостей, управління ризиками, правові аспекти кібербезпеки тощо) на реальних прикладах.

Формат занять

Індивідуальне завдання (звіт, щоденник практики), консультації. Підсумковий контроль – залік.

Компетентності

- ЗК1. Здатність застосовувати знання у практичних ситуаціях.
- ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
- ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
- ЗК1. Здатність застосовувати знання у практичних ситуаціях.
- ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
- ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
- СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
- СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
- СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
- СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

- РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
- РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
- РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
- РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
- РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
- РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
- РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

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)

Комплексні системи захисту інформації, Безпека інтернет-речей, Веббезпека, Комплексний тренінг, Антивірусний захист інформації, Основи машинного навчання для кібербезпеки.

Особливості освітнього компонента, методи та технології навчання

В ході проходження виробничої практики викладачами-керівниками застосовуються методичні рекомендації. В якості методів викладання, які направлені на активізацію, стимулювання та контроль навчально-практичної діяльності здобувачів, застосовуються консультаційні зустрічі.

Тематика індивідуального завдання

Тематика визначається з урахуванням місця практики за згодою керівників від навчального закладу та місця проходження практики, також в методичних рекомендаціях представляються основні напрями індивідуального завдання.

Література та навчальні матеріали

1. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ: ДП “УкрНДНЦ”, 2016. – 17 с. URL: <https://pdf.lib.vntu.edu.ua/books/2018/%D0%94%D0%A1%D0%A2%D0%A3%208302%20%D0%BF%D0%BE%D0%B2%D0%BD%D0%B8%D0%B9.pdf>
2. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ: ДП “УкрНДНЦ”, 2016. – 31 с. URL: https://science.kname.edu.ua/images/dok/derzhstandart_3008_2015.pdf
3. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ: ДП “УкрНДНЦ”, 2015. – 65 с. URL: https://udhtu.edu.ua/wp-content/uploads/2018/03/DSTY_1_5_2015.pdf
4. Данильян О. Г. Дзьобань О. П. Методологія наукових досліджень: підручник – Харків: Право, 2019. – 368 с. URL: https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf

Додаткова література :

1. Закон України “Про національну безпеку”. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
2. Закон України “Про захист персональних даних”. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481/ URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
3. Чмиленко Ф.О., Жук Л.П. Посібник до вивчення дисципліни «Методологія та організація наукових досліджень» – Дніпро: РВВ ДНУ, 2014. – 48 с. URL: <http://kist.ntu.edu.ua/textPhD/mond.pdf>
4. Методологія і організація наукових досліджень. [текст]: навч. посіб. / Г.О. Бірта, Ю.Г. Бургу– Київ: «Центр учбової літератури», 2014. – 142с. URL: <http://dspace.puet.edu.ua/bitstream/123456789/10160/1/978-620-0-61809-2.pdf>

Система оцінювання

Критерії оцінювання успішності здобувача та розподіл балів

Опис структури підсумкової оцінки, обов'язкових завдань та процедури нарахування балів, особливо звертаючи увагу на самостійну роботу та індивідуальні завдання.

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: https://blogs.kpi.kharkov.ua/v2/nv/?page_id=208

Погодження

Силабус погоджено

30.08.2025



Завідувач кафедри
Сергій ЄВСЄЄВ

30.08.2025



Гарант ОП
Сергій ЄВСЄЄВ