



Силабус освітнього компонента Програма практики



Виробнича практика

Шифр та назва спеціальності

K4 – Управління інформаційною безпекою

Спеціалізація

-

Освітня програма

Управління інформаційною безпекою

Рівень освіти

Перший (бакалаврський)

Семестр

6

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Кафедра

Кібербезпеки (328)

Тип освітнього компонента

Практична, Обов'язкова

Форма навчання

Денна

Мова викладання

Українська

Розробники

**СВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.

Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп'ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

[Детальніше про викладача на сайті кафедри](#)



КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу», «Безпека та аудит бездротових та рухомих мереж», гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)



ГАВРИЛОВА Алла Андріївна

alla.havrylova@khp.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

Виробнича практика є нормативною складовою підготовки бакалаврів. Виробнича практика спрямована на формування у студентів навичок щодо підсумовування теоретичної та практичної підготовки з управління інформаційною безпекою

Мета та завдання

Отримання студентами необхідних знань щодо 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/іспит.

Компетентності

ЗК1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК2. 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.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність спілкуватися іноземною мовою.

СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.

СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

РН2. Вміти використовувати 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.

РН4. Вільно спілкуватися державною мовою.

РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН-13. Вміти вирішувати задачі забезпечення та супроводу (в т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

РН17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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)

Математичні основи криптології та криптоаналіз, Основи криптографічного захисту, Моделювання систем критичної інфраструктури, Менеджмент інформаційної безпеки, Основи соціальної інженерії, Введення в мережі, Основи стеганографічного захисту інформації, Цифрова криміналістика, Правове регулювання кібербезпеки, Організація документообігу з обмеженим доступом, Безпека смарт-технологій та Інтернет-речей, Промисловий та офісний шпіонаж, Веб безпека, Антивірусний захист інформації.

Особливості освітнього компонента, методи та технології навчання

Математичні основи криптології та криптоаналіз, Основи криптографічного захисту, Моделювання систем критичної інфраструктури, Менеджмент інформаційної безпеки, Основи соціальної інженерії, Введення в мережі, Інтернетика. Теорія пошуку. Моделі та алгоритми, Цифрова криміналістика, Правове регулювання кібербезпеки, Організація документообігу з обмеженим доступом, Блокчейн та смарт-технології в електронному документообігу, Національні інформаційні ресурси, Веб безпека, Антивірусний захист інформації.

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

Основна література:

1. Edited by Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: <http://webcache.googleusercontent.com/search?q=cache:Ii4pGrNeP2QJ:www.repository.hneu.edu.ua/jspui/handle/123456789/25623+&cd=1&hl=ru&ct=clnk&gl=ua>.
2. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. DOI: [10.15587/978-617-7319-72-5](https://doi.org/10.15587/978-617-7319-72-5).
3. Edited by Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych, Volodymyr Hrytsyk, Oleksandr Milov, Olha Korol, Stanislav Milevskyi, Roman Korolev, Serhii Pohasii, Andrii Tkachov, Yevgen Melenti, Oleksandr Lavrut, Alla Havrylova, Serhii Herasymov, Halyna Holotaistrova, Dmytro Avramenko, Roman Vozniak, Oleksandr Voitko, Kseniia Yerhidgei, Serhii Mykus, Yurii Pribyliev, Olena Akhiezer, Mykhailo Shyshkin, Ivan Oprisky, Oleh Harasymchuk, Olha Mykhaylova, Yuriy Nakonechnyy, Marta Stakhiv,

Bogdan Tomashevsky 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: <http://monograph.com.ua/catalog/book/978-617-7319-57-2>.

4. Технології захисту інформації. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. URL: <http://kist.ntu.edu.ua/textPhD/tzi.pdf>.

6. Методичні вказівки до проведення виробничої практики [Електронний ресурс] : для студентів першого (бакалаврського) рівня вищої освіти за спец. 125 "Кібербезпека та захист інформації" / уклад.: С. П. Євсєєв, О. Г. Король, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2024. – 22 с. – URI: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/81233>.

Додаткова література :

1. Havrylova A., Khokhlachova Y., Tkachov A., Voropay N., Khvostenko V. Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journa. 2023, Vol. 25, №. 1. P. 6-19. URL: <https://doi.org/10.18372/2410-7840.25.17593>.
2. Yevseiev S., Havrylova A., Milevskyi S., Sinitsyn I. and others. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023, № 3/9 (123). P. 33-48. DOI: [10.15587/1729-4061.2023.281795/](https://doi.org/10.15587/1729-4061.2023.281795/)
3. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсєєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. – Львів: «Новий Світ- 2000», 2020. – 196 с. URL: <http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/pdf2.pdf>
4. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020. – 241 с. URL: <http://repository.hneu.edu.ua/handle/123456789/24508>
5. Євсєєв С.П., Дженюк Н.В., Охрименко М.Ю., Головашич С.О., Кудій Д.А. Е25 Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсєєв С. П., Дженюк Н.В., Охрименко М.Ю. та ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 513 с. URL: <https://ns2000.com.ua/tsyfrova-skhemotekhnika-ta-arkhitektura-mikroprotsesoriv-navchalnyy-posibnyk/>.

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 ЄВСЕЄВ

30.08.2025



Гарант ОП

Роман КОРОЛЬОВ