Силабус освітнього компонента

Програма практики

Науково-дослідницька практика

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип освітнього компонента
Практична підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
4

Мова викладання
Українська

Розробники

ЄВСЕЄВ 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 статтей 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

МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проєктами» у студентів бакалавріата та магістратури, «Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у 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 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 ІТ-проєктами та їх безпека» у студентів бакалавріату
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Направлена на формування ключових фахових компетентностей, які неможливо повноцінно здобути в аудиторії, до складу яких входять: аналітичні навички: вміння аналізувати вразливості, виявляти загрози та оцінювати ризики для конкретної інфраструктури; навички роботи з інструментами: освоєння професійного програмного забезпечення та обладнання, що використовується для моніторингу, захисту й аналізу безпеки; м'які навички (soft skills): робота в команді, ефективна комунікація з колегами та керівництвом, відповідальність і вміння працювати в умовах стресу

Мета та завдання

Закріплення, поглиблення та систематизація знань, отриманих під час навчання, що дає змогу здобувачам набути практичного досвіду у розв'язанні реальних завдань у сфері кібербезпеки, освоїти сучасні методи та інструменти для захисту інформаційних систем, даних і мереж, сформувати навички аналізу ризиків, розроблення та впровадження політик безпеки, зібрати, обробити та проаналізувати матеріали, необхідні для написання кваліфікаційної магістерської роботи та розвинути професійні компетенції, включаючи критичне мислення, вміння працювати в команді та самостійно приймати рішення в умовах, що постійно змінюються.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-
математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до
персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг освітнього компонента

Загальний обсяг дисципліни – 570 год. (19 кредитів ECTS): самостійна робота – 570 год.

Тривалість практики

Тривалість практики – 7 тижнів.

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 науково-дослідної 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. Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. для здобувачів ступеня магістра за освітніми програми Комп'ютерні системи і технології спеціального зв'язку та Спеціальні системи електронних комунікацій спец. 122 Комп'ютерні науки 172 Електронні комунікації та радіотехніка / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,73 Мбайт). – Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. – 140 с. https://ela.kpi.ua/server/api/core/bitstreams/c4ad5148-9e04-4979-9ef7-0fec3a385650/content
2. Чунарьова А., Чунарьов А. Система управління інформаційною безпекоюна базі міжнародних стандартів серії ISO. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. С. 48 - 52.
3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с. https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf

4. Григор'єв В. І. Інформаційні загрози в державному управлінні // Наукові записки Львів. ун-ту бізнесу та права. 2013. Вип. 11. С. 93. URL: http://irbis-nbuv.gov.ua/UJRN/Nzlubp_2013_11_26
5. Терещенко, Л. (2021). Управління ризиками інформаційних систем: етапи процесу управління ризиками. Економіка та суспільство, (31). https://doi.org/10.32782/2524-0072/2021-31-12
6. Кіберризики критичної інфраструктури: від аналізу загроз до впровадження рішень [Текст] : наук.- практ. посіб. / Олександр Довгань, Тарас Ткачук ; Держ. наук. установа "Ін-т інформації, безпеки і права Нац. акад. прав. наук України". - Київ ; Одеса : Фенікс, 2024. - 70 с. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=JwU_B&S21ALL=%28%3C.%3EI%3D%21NBUV$%3C.%3E%29%2A%28%3C.%3EU%3D%D0%A5849%284%D0%A3%D0%9A%D0%A0%2904:%D0%9797%3C.%3E%29&Z21ID=&S21SRW=TIPVID&S21SRD=DOWN&S21STN=1&S21REF=10&S21CNR=20
7. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві [Електронний ресурс] / З. Свердлик // Український журнал з бібліотекознавства та інформаційних наук. - 2022. - Вип. 10. - С. 175-188. - URL: http://nbuv.gov.ua/UJRN/ujlis_2022_10_17
8. Дорошенко А. Захист персональних даних у сфері Data Science: імплементація GDPR в Україні [Текст] : [монографія] ; "Erasmus+" Programme of the European Union ; [Нац. ун-т "Львів. політехніка"]. Львів : Вид-во Тараса Сороки, 2022. С. 80-88. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=JwU_B&S21ALL=%28%3C.%3EI%3D%21NBUV$%3C.%3E%29%2A%28%3C.%3EU%3D%D0%A5849%284%D0%A3%D0%9A%D0%A0%2904:%D0%9797%3C.%3E%29&Z21ID=&S21SRW=TIPVID&S21SRD=DOWN&S21STN=1&S21REF=10&S21CNR=20
9. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи та засоби убезпечення. Системи управління інформаційною безпекою. Вимоги. Київ : Держстандарт України, 2015. 48 с. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf
10. Загальний регламент про захист даних (GDPR) : Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 13.07.2025).
11. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. С. 138–150. URL: https://zakon.rada.gov.ua/laws/main/2163-19#Text
12. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 18.08.2025).
13. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 13.07.2025).
14. Зубенко С. В., Ракша О. В. Мережева безпека : навч. посіб. Київ: ІТНВУ, 2019. 256 с. URL: https://elartu.tntu.edu.ua/bitstream/lib/42625/1/%D0%9A%D0%91%D0%86%D0%9C%D0%A1_%28%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%29.pdf
15. Ігнатенко Р. С. Захист вебдодатків від DDoS-атак: сучасні підходи. Наукові праці Інституту кібербезпеки. 2023. Вип. 1 (45). С. 112-120. https://dspace.onua.edu.ua/server/api/core/bitstreams/cf6c1f9c-b1d7-4c35-9b35-2e8901b23fdd/content
16. Кіберзахист в умовах гібридної війни: монографія. / за заг. ред. О. В. Довгаля. Харків : ТОВ "Видавництво "Нове слово", 2021. 288 с. https://dnuvs.ukr.education/wp-content/uploads/2025/06/zbirnyk_materialiv_17_kvitnya_2025_compressed.pdf
17. Когут О. В. Міжнародна кібербезпека: виклики та співпраця : навч. посіб. Львів : ЛНУ ім. І. Франка, 2021. 250 с. https://nashformat.ua/pdf-preview/kiberbezpeka-ta-ryzyky-tsyfrovoi-transformatsii-kompanij-928039?srsltid=AfmBOooeyaQ8Rvb_BP4tDNenSGt8YafubMbe5FXGCCJgljORK3kdewOk
18. Козаченко Ю. М., Мельник О. М. Застосування машинного навчання для виявлення аномалій у мережевому трафіку. Вісник кібербезпеки. 2023. № 2. С. 45–56. URL: https://indico.ldubgd.edu.ua/event/55/attachments/662/975/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%B8%D1%85%20%D0%BF%D1%80%D0%B0%D1%86%D1%8C%20%D0%BA%D0%BE%D0%BD%D1%84.%

20%D0%86%D0%91%D0%86%D0%A2_2024%20%E2%80%93%20%D0%B7%20%D0%BE%D0%B1%D0%BA%D0%BB%D0%B0%D0%B4%D0%B8%D0%BD%D0%BA%D0%BE%D1%8E.pdf
19. Кривогуз І. М. Криптографічні методи захисту інформації. Львів : Видавництво Львівської політехніки, 2019. 250 с. https://vaodesa.mil.gov.ua/wp-content/uploads/2024/10/Zbirnyk-tez-dop.-Nats.-bezpeka-Ukrainy-aktualny-problemy-ta-shliakhy-ikh-vyrishennia-1.pdf
20. Ліщук В. В. Аналіз сучасних кіберзагроз в умовах гібридної війни. Інформаційна безпека. 2024. Т. 1, № 1. С. 110–125. https://hups.mil.gov.ua/assets/doc/science/conference/20/xx-conf-hnups_01.pdf
21. Павленко О. В. Аналіз сучасних методів кіберрозвідки та протидія цілеспрямованим атакам. Проблеми кібербезпеки. 2024. № 1 (25). С. 45-53. https://archer.chnu.edu.ua/bitstream/handle/123456789/12135/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%202024%20%D0%A8%D1%82%D1%83%D1%82%D0%B3%D0%B0%D1%80%D1%82.pdf?sequence=1&isAllowed=y
22. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки : навчальний посібник [електронний ресурс]. Дніпро, 2023. – 200 с. URL: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
23. Потопальський В. В., Лисенко О. А., Семенов І. Г. Захист інформації: криптографічні методи. Київ : Центр навчальної літератури, 2022. 356 с. https://kingu.edu.ua/wp-content/
uploads/2024/0
7/%D0%97%D0%91%D0%86%
D0%A0%D0%9D%D0%98%D0%9A-%D1%82%D0%B5%D0%B7-
%D0%B4%D0%
BE%D0%BF%D0%BE%D0%B2
%D1%96%D0%B4%D0%B5%D0%B9-%D0%9D%D0%9F%D0
%9A-%D0%A4%D0%A1%D0%91%D0%94-%D0%9
D%D0%93%D0%A3.pdf
24. Скляров В. А. Безпека програмного забезпечення та даних : навч. посіб. Харків : Ранок, 2023. 360 с.
25. Адамов О. С. Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням машинного навчання [Текст] : автореф. дис. ... канд. техн. наук : 05.13.05 /; Харк. нац. ун-т радіоел. Харків, 2019. 31 с. : рис., табл. URL:
https://openarchive.nure.ua/server/api/core/bitstreams/529a9e7c-069c-4bd3-99ea-7398e7a33fef/content
26. Щеголенкова Н. М. Аудит інформаційної безпеки: навч. посіб. Львів: Магнолія Плюс, 2022. 280 с. URL:
https://www.google.com/aclk?sa=L&pf=1&ai=DChsSEwjqzrft2bCPAxUrCqIDHbEjPIwYACICCAEQABoCbGU&co=1&ase=2&gclid=EAIaIQobChMI6s637dmwjwMVKwqiAx2xIzyMEAAYASAAEgI5ofD_BwE&cid=CASJeRo3OkjayRwsRDY_jpGtCfajHPsE0gvNn3awsbidorNbK9lv8k&cce=2&category=acrcp_v1_32&sig=AOD64_1uxFNtInYWktpiHObyogUgj-DKAg&q&nis=4&adurl=https://xray-sec.com/ua/?utm_source%3Dgoogle%26utm_medium%3Dcpc%26utm_campaign%3Dsearch-ua-ukr%26utm_term%3Daudit-ib%26gad_source%3D1%26gad_campaignid%3D21032544132%26gbraid%3D0AAAAAqc6yf5THn0dBnvDeIZ2_FWNWLB4U%26gclid%3DEAIaIQobChMI6s637dmwjwMVKwqiAx2xIzyMEAAYASAAEgI5ofD_BwE&ved=2ahUKEwjXmLDt2bCPAxW5QVUIHXpFAIoQ0Qx6BAgYEAE
27. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. 2022. Вип. 44. DOI: https://doi.org/10.32782/2524- 0072/2022-44-21.
28. CERT-UA. Річний звіт про кіберінциденти у 2023 році. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/article/11223 (дата звернення: 17.08.2025).
29. CERT-UA. Звіт про кіберінциденти та кібератаки на об'єкти критичної інфраструктури України. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/reports (дата звернення: 18.08.2025).
30. ENISA Threat Landscape Report 2023. European Union Agency for Cybersecurity (ENISA). 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 18.08.2025).
31. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. URL: https://www.iso.org/standard/82875.html (access on: 18.08.2025).
32. Kaspersky Security Bulletin. Statistics 2024. Kaspersky. 2024. URL:
https://www.kaspersky.com/about/security-bulletin (access on: 18.08.2025).

33. Microsoft. Digital Defense Report 2024. URL: https://www.microsoft.com/en-us/security/business/reports/digital-defense-report-2024 (acces on: 17.08.2025).
34. Modeling of security systems for critical infrastructure facilities [Text] : monograph / [R. Korolev et al.] ; ed. by Serhii Yevseiev [et al.]. Kharkiv : PC Technology Center, 2022. XIV, P. 169-181. https://doi.org/10.15587/978-617-7319-57-2
35. NIST Cybersecurity Framework (National Institute of Standards and Technology Cybersecurity Framework). URL: https://www.nist.gov/cyberframework (acces on: 13.07.2025).
36. Simpson Michael T., Antill Nicholas, Backman Kent. Hands-On Ethical Hacking and Network Defense. Boston: Cengage Learning, 2022. 720 p. URL: https://books.google.com.ua/books/about/Hands_On_Ethical_Hacking_and_Network_Def.html?id=S1RbzgEACAAJ&redir_esc=y

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** Станіслав МІЛЕВСЬКИЙ