



Силабус освітнього компонента Програма практики



Переддипломна практика

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Освітньо-професійна програма Кібербезпека

Кафедра

Кібербезпеки (328)

Рівень освіти

Магістр

Тип освітнього компонента

Практична підготовка, Обов'язкова

Семестр

3

Мова викладання

Українська

Розробники

**ЄВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpі.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](#)

**КОРОЛЬ Ольга Григорівна**

olha.korol@khpі.edu.ua

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

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави», «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків», у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua

кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-наукової програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



ГАВРИЛОВА Ааврилова 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: «Презентація та обробка знань», «Безпека та анонімність роботи в Інтернеті», «Переддипломна практика» та «Науково-дослідна практика» у студентів магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Переддипломна практика проводиться після закінчення теоретичного навчання і складання всіх заліків і іспитів та є заключним етапом навчання студентів другого рівня вищої освіти «Магістр». Переддипломна практика повинна розширити і поглибити теоретичні та практичні знання за освітньою програмою, отримані при навчанні, закріпити здобуті вміння та навички у сфері інформаційної та/або кібербезпеки, сприяє набуттю студентом особистісних і професійних компетентностей, пов'язаних із проведенням наукових досліджень, оформленням і публікацією отриманих наукових результатів, прийняттям професійних рішень, збір, аналіз і підготовку матеріалів для написання кваліфікаційної (магістерської) роботи.

Мета та завдання

Узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профільними дисциплінами, що вивчені, за спеціальністю "Кібербезпека та захист інформації", отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз та розроблення плану кіберзахисту інформаційної системи. Отримані під час практики знання та досвід дозволять студентам якісно підготувати кваліфікаційну роботу, а також підвищити їхню професійну компетентність у сфері кібербезпеки.

Формат занять

Самостійна робота, 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.

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. Проводити 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 напрямку 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.

Обсяг освітнього компонента

Загальний обсяг дисципліни – 360 год. (12 кредитів ECTS): самостійна робота – 360 год.

Тривалість практики

Тривалість практики – 6 тижнів.

Передумови освітнього компонента (пререквізити)

Для успішного проходження переддипломної практики необхідно мати знання та практичні навички зі всіх обов'язкових дисциплін освітньої програми.

Особливості освітнього компонента, методи та технології навчання

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

Студенти можуть проходити переддипломну практику на підприємствах і в організаціях різних галузей, а також на кафедрі кібербезпеки НТУ «ХПІ». У разі проходження практики в НТУ «ХПІ» керівництво практикою здійснюється керівником від кафедри кібербезпеки. У випадку проходження практики на підприємствах (організаціях, установах) призначаються керівники практики від випускової кафедри та від відповідного підприємства або організації, на якому студент проходитиме практику. Перед початком практики студент отримує настанови від керівника практики від випускової кафедри, обговорює цілі і завдання практики, тему кваліфікаційної роботи і індивідуальне завдання на практику.

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. Аналіз загроз кібербезпеки та розробка засобів їх нейтралізації.

Тематика 2. Моніторинг та аналіз кіберінцидентів у корпоративних мережах.

Тематика 3. Захист даних у хмарних середовищах.

Тематика 4. Методи та засоби криптографічного захисту інформації.

Тематика 5. Оцінка вразливостей веб-додатків та методи їх захисту.

Тематика 6. Розробка та впровадження політик інформаційної безпеки в організаціях.

Тематика 7. Системи багатофакторної автентифікації та їх застосування в корпоративних мережах.

Тематика 8. Захист інформаційних систем від внутрішніх загроз.

Тематика 9. Застосування штучного інтелекту для виявлення та протидії кіберзагрозам.

Тематика 10. Захист мобільних додатків та платформ.

Література та навчальні матеріали

Основна література

1. Методичні вказівки до проведення практики за другим (магістерським) рівнем для студентів спеціальності 125 “Кібербезпека та захист інформації” / уклад. Н. І. Воропай, О. В. Мілов, О. Г. Король, Н. І. Воропай. – Харків: НТУ “ХПІ”. – 28 с. URL:

<https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0b9f7a2c-7b44-4f86-b061-f2e677428f8c/content>

2. 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

3. 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

4. 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>

5. 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

6. 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

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. Чмиленко Ф.О., Жук Л.П. Посібник до вивчення дисципліни «Методологія та організація наукових досліджень» – Дніпро: РВВ ДНУ, 2014. – 48 с.
<http://kist.ntu.edu.ua/textPhD/mond.pdf>

10. Методологія і організація наукових досліджень. [текст]: навч. посіб. / Г.О. Бірта, Ю.Г. Бургу–Київ: «Центр учбової літератури», 2014. – 142с.
https://shron1.chtyvo.org.ua/Burhu_Yurii/Metodolohiia_i_orhanizatsiia_naukovykh_doslidzhen.pdf

11. 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>.

12. 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.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

13. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020. – 241 с.
<http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf>
14. 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.
https://drive.google.com/file/d/1fTWf7v4v-aaCL_oHMSHsyIJOrNIEu9v-/view
15. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] // База даних "Законодавство України" / ВР України. – Режим доступу до журн. : <http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741> 483 (дата звернення: 10.04.2018).
16. Данильян О. Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с.
https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf
17. Інформаційна безпека та інформаційні технології. – Х.; ТОВ "ДІСА ПЛЮС", 2019. - 322 с.
http://library.kpi.kharkov.ua/files/new_postupleniya/ibtait.pdf
18. Управління бізнес-процесами: Навч. посібник. – Рівне: НУВГП, 2014. – 158 с.
<https://ep3.nuwm.edu.ua/8812/1/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%20%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%B0%D0%BC%D0%B8.pdf>
19. Женченко М. Загальна і спеціальна бібліографія: навч. посіб. / М. Женченко. – Київ : Жнець, 2011. – 255 с.
<http://lib-hdak.in.ua/new-acquisitions-archive/new-acq-1-2012/68-bibliography.html>
20. Security Cloud [Електронний ресурс]. – Режим доступу :
<https://www.cisco.com/site/us/en/products/security/security-cloud/index.html>
21. Kali Linux [Електронний ресурс]. – Режим доступу : <https://www.kali.org/>.
22. James Kurose, Keith Ross, Computer Networking: A Top-Down Approach.
https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20%20A%20Top%20Down%20Approach.%207th.%20converted.pdf
23. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.
<https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf>
24. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша - К.: ВБ «Аванпост-Прим», 2012.-214 с. [Електронний ресурс].- Режим доступу:
https://www.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/article/12058.016.pdf
25. Borova T. English for Business Analysts: textbook: in 3 parts, Part 3. Business Intelligent Tools / T. Borova, O. Milov. – Kharkiv: S. Kuznets KhNUE, 2018. – 179 P. [Електронний ресурс].- Режим доступу:
<http://repository.hneu.edu.ua/bitstream/123456789/21467/1/2018-%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%B0%20%D0%A2%20%D0%90%2C%20%D0%9C%D1%96%D0%BB%D0%BE%D0%B2%20%D0%9E%20%D0%92.pdf>
26. Котлубай В. О. Інноваційне підприємництво та управління стартап проектами. Economic evaluation of innovative solution : практикум / В. О. Котлубай, Г. А. Отливанська. – Одеса : НУ "ОЮА", 2021. – 131 с. [Електронний ресурс]. – Режим доступу:
<https://dspace.onua.edu.ua/server/api/core/bitstreams/dbd21a89-cc80-479b-9f28-17b4d8998767/content>
27. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p. 2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p. [Електронний ресурс]. – Режим доступу:
<https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf>
28. Баранов А.А., Интернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с. [Електронний ресурс]. – Режим доступу:
<https://pravo-izdat.com.ua/image/data/Files/476/3 Internet rechej Tom I vnutri.pdf>
29. Словник книгознавчих термінів / уклад.: В. Я. Буран, В. М. Медведєва, Г. І. Ковальчук, М. І. Сенченко. – Київ : Аратта, 2003. – 160 с.
<https://ube.nlu.org.ua/article/%D0%92%D0%B0%D0%BA%D0%B0%D1%82%D0%B0>

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

28.08.2024



Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП

Ольга КОРОЛЬ