Силабус освітнього компонента
Програма практики

Науково-дослідницька практика

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип освітнього компонента
Практична підготовка, Обов'язковий

Семестр
4

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

КОРОЛЬ Ольга Григорівна

olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статтей 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

ГАВРИЛОВАаврилова 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

Науково-дослідницька практика проводиться після закінчення теоретичного навчання і складання всіх заліків і іспитів та є заключним етапом навчання студентів за освітньо-науковою програмою "Кібербезпека" другого рівня вищої освіти "Магістр". Науково-дослідницька практика магістрів спеціальності "Кібербезпека та захист інформації" спрямована на розвиток науково-дослідницьких навичок та вдосконалення підготовки студентів до проведення самостійних досліджень у сфері кібербезпеки. Цей вид практики дозволяє студентам поглибити свої знання у вибраній тематиці дослідження, розробити власні наукові проекти та отримати практичний досвід застосування сучасних методів і технологій для вирішення актуальних завдань в області інформаційної безпеки.

Мета та завдання

Метою науково-дослідної практики є формування у студентів навичок проведення наукових досліджень у галузі кібербезпеки та захисту інформації. Практика спрямована на те, щоб студенти освоїли методи проведення наукових досліджень та підготовки наукових публікацій, розвинули вміння формулювати гіпотези, розробляти дослідницькі плани та проводити експериментальні дослідження, поглибили свої знання у вибраних напрямах кібербезпеки, таких як криптографія, аналіз вразливостей, захист мережевих інфраструктур, аналіз кіберзагроз тощо.
Отримали досвід впровадження наукових розробок у практику та розробки рішень, які можна використовувати для захисту інформаційних систем, підготували науковий звіт, що стане основою для подальшої підготовки магістерської роботи або публікацій. Вивчення теоретичних проблем у рамках програми магістерської підготовки та проведення аналізу об’єкту дослідження відповідно до теми магістерської роботи.

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.
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 – 10 тижнів.

Передумови освітнього компонента (пререквізити)

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

Особливості освітнього компонента, методи та технології навчання

Науково-дослідницька практика магістрів за спеціальністю "Кібербезпека та захист інформації" відрізняється високим рівнем спеціалізації та орієнтацією на вирішення актуальних проблем інформаційної безпеки в сучасних умовах.
Основні особливості цієї практики включають:
1. Глибокий аналітичний підхід - студенти проводять детальний аналіз сучасних загроз кібербезпеки, вивчають існуючі наукові дослідження та використовують отримані знання для проведення власних досліджень.
2. Індивідуалізація тематики досліджень - кожен студент обирає тему для дослідження, що відповідає його науковим інтересам та напрямкам майбутньої магістерської роботи. Тематика дослідження може бути пов'язана з новими технологіями захисту, кіберзагрозами або новими методами аналізу й оцінки ризиків у системах інформаційної безпеки.
3. Реальна наукова робота - студенти мають змогу працювати з реальними даними, інфраструктурою або сценаріями, що дозволяє їм розробляти практично значущі рішення для вирішення проблем кібербезпеки.
4. Міждисциплінарний підхід - оскільки кібербезпека є багатогранною дисципліною, практика часто вимагає застосування знань з суміжних галузей, таких як програмування, криптографія, аналітика, машинне навчання, управління ризиками, а також правові та етичні аспекти захисту інформації.
5. Робота з новітніми технологіями та засобами захисту - студенти мають можливість використовувати сучасні програмні та апаратні засоби для захисту інформації, такі як системи виявлення вторгнень (IDS/IPS), інструменти для аналізу трафіку, засоби шифрування та методи тестування на проникнення (penetration testing).
Методи та технології навчання під час науково-дослідницької практики:
1. Методи проектної роботи - студенти працюють над реальними проектами, що мають наукову або прикладну цінність. Кожен студент може самостійно обрати напрямок досліджень, формулювати гіпотези та розробляти наукові підходи до їх вирішення.
2. Метод наукового експерименту - науково-дослідна практика включає проведення експериментів, моделювання атак на інформаційні системи або тестування засобів захисту. Це дозволяє студентам оцінити ефективність методів захисту на основі практичних даних.

3. Інтерактивне навчання - в процесі практики студенти можуть брати участь у наукових семінарах, конференціях та воркшопах, де обговорюються новітні досягнення в галузі кібербезпеки. Це сприяє обміну знаннями та отриманню досвіду з актуальних проблем галузі.
4. Самостійне дослідження - під час практики студентам надається можливість самостійно проводити дослідження, здійснювати пошук інформації, аналіз літератури, а також формулювати висновки та пропозиції щодо вирішення кібербезпекових проблем.
5. Використання сучасних програмних засобів - для дослідження та моделювання студентам надаються програмні інструменти для аналізу кіберзагроз, тестування захисту інформаційних систем, моніторингу мережевого трафіку та криптографічних протоколів (наприклад, Wireshark, Metasploit, Nessus, Burp Suite, та інші).
6. Метод аналізу та синтезу - студенти вчаться збирати інформацію з різних джерел, здійснювати критичний аналіз наукових досліджень та застосовувати отримані дані для розробки нових рішень. Синтез нових знань дозволяє краще розуміти сучасні виклики в сфері кібербезпеки.
7. Технології дистанційного навчання - в умовах сучасного інформаційного середовища, студенти можуть використовувати різні онлайн-платформи для доступу до наукових ресурсів, проведення вебінарів, а також комунікації з науковими керівниками.
Застосування цих методів навчання сприяє розвитку у студентів критичного мислення, аналітичних навичок, а також вміння самостійно проводити наукові дослідження в умовах швидкої зміни технологічного середовища.
Студенти можуть проходити науково-дослідницьку практику на підприємствах і в організаціях різних галузей, а також на кафедрі кібербезпека НТУ "ХПІ". У разі проходження практики в НТУ «ХПІ» керівництво практикою здійснюється керівником від кафедри кібербезпека. 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 науково-дослідницької практики:
Тематика 1. Розробка системи виявлення та запобігання кіберзагрозам на основі машинного навчання.
Тематика 2. Оцінка ризиків кібербезпеки для хмарних обчислювальних платформ.
Тематика 3. Аналіз захищеності корпоративних мережевих систем від внутрішніх загроз.
Тематика 4. Моделювання та аналіз атак на веб-додатки: методи та засоби захисту.
Тематика 5. Криптографічні методи захисту даних у розподілених системах.
Тематика 6. Оцінка ефективності засобів багатофакторної автентифікації у корпоративних системах.
Тематика 7. Захист промислових систем управління (ICS/SCADA) від кіберзагроз.
Тематика 8. Розробка політики інформаційної безпеки для малих та середніх підприємств (SME).
Тематика 9. Захист мобільних додатків від атак: аналіз вразливостей та розробка рекомендацій.
Тематика 10. Аналіз ефективності сучасних засобів тестування на проникнення (Penetration Testing).
Тематика 11. Застосування штучного інтелекту для моніторингу кіберзагроз у реальному часі.
Тематика 12. Методи шифрування та захисту конфіденційної інформації у фінансових транзакціях.
Тематика 13. Дослідження вразливостей у мережах Інтернету речей (IoT) та їх захист.
Тематика 14. Оцінка ефективності систем виявлення та попередження атак на базі великих даних (Big Data).
Тематика 15. Правові та етичні аспекти кібербезпеки: впровадження стандартів захисту інформації.

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. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с. URL: https://duikt.edu.ua/ua/lib/1/category/2404/view/1242
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с. URL: https://duikt.edu.ua/uploads/p_303_92597962.pdf
5. Гудмен М. Злочини майбутнього / М. Гудмен ; пер. з англ.: І. Мазарчук, Я. Машико. – Харків : Ранок : Фабула, 2019. – 592 с. URL: https://library.nlu.edu.ua/novi-nadkhodzhennia/item/3095-zlochyny-maibutnoho.html
6. Юлія Лісовська, Кібербезпека. Ризики та заходи. К.: Кондор , 2019 , 272с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf
7. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: Навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с. URL: http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf

8. В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Захист систем електронних комунікацій , Видавництво: КНТЕУ – 2019, Стор.164, ISBN: 978-966-629-970-6. URL: https://knute.edu.ua/file/MjkwMjQ=/b6f7ccc72573e35b6f930d8f11f65c51.pdf
9. М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; Інформаційна безпека. Підручник В. В. Остроухов, під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с. URL: https://lira-k.com.ua/preview/12867.pdf
10. 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
11. 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
12. 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
13. 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
14. 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.
15. 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

16. 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.
17. 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
18. 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
19. 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.
20. Технологія Ethernet: лабораторний практикум / М. О. Білова, С. П. Євсеєв, 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.
21. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, 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
22. Євсеєв С.П., Дженюк Н.В., Охрименко М.Ю., Головашич С.О., Кудій Д.А. Е25 Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсеєв 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_oHMSHsyIJOrNlEu9v-/view
23. 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).
24. 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
25. Інформаційна безпека та інформаційні технології. – Х.; ТОВ “ДІСА ПЛЮС”, 2019. - 322 с.

http://library.kpi.kharkov.ua/files/new_postupleniya/ibtait.pdf
26. 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
27. 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
28. Security Cloud [Електронний ресурс]. – Режим доступу : https://www.cisco.com/site/us/en/products/security/security-cloud/index.html
29. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/.
30. 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
31. 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
32. 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
33. 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
34. 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
35. Бобало Ю. Я., Дудикевич В. Б., Микитин Г. В. Стратегічна безпека системи “об’єкт – інформаційна технологія” , Видавництво: Львівська політехніка = 2020, Стор.: 260, ISBN: 978- 966-941-481-6. URL: https://ena.lpnu.ua/items/5df4d5d1-9e93-4a17-8d6d-15242a88defa
36. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: Навч. посібник. Дніпро: Дніпроп. держ. Унт внутріш. справ, 2020. 144 с. URL: https://duikt.edu.ua/ua/lib/1/category/1195/view/486
37. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
38. Когут Ю.І., Кібербезпека та ризики цифрової трансформації компаній : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. – 372 с. URL: https://kniga.biz.ua/pdf/31947-kiberbezpeka-1.pdf?srsltid=AfmBOoq--yrf1PNzB2vSfgUaMWofyfNRE-kSwPsQnpXinyG7NKrcP5Fs
39. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO Видавництво: Львівська політехніка Рік видання: 2021, С.: 232, ISBN: 978-966-941-583-7. URL: https://vlp.com.ua/node/20266
40. Когут Ю. І., Кібертероризм (історія, цілі, об’єкти) : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2023. – 304 с. URL: https://jurkniga.ua/contents/kiberterorizm-istoriya-tsili-obiekti-praktichniy-posibnik.pdf
41. Положення про проведення практики студентів вищих навчальних закладів України URL: https://zakon.rada.gov.ua/laws/show/z0035-93#Text.
42. Закон України «Про інформацію» від 02.10.1992 No 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
43. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

44. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційнотелекомунікаційних системах» від 29.03.2006 No373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
45. 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
46. Баранов А.А., Інтернет 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
47. 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
48. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
49. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf
50. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації. URL: https://tzi.com.ua/downloads/2.6-001-11.pdf
51. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
52. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-010-03.pdf
53. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.7-009-09.pdf
54. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. URL: https://tzi.com.ua/downloads/2.7-011-2012.pdf
55. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи. URL:
https://tzi.com.ua/downloads/3.1-001-07.pdf
56. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. URL: https://tzi.com.ua/downloads/3.3-001-07.pdf
57. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/3.6-001-2000.pdf
58. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

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 Станіслав МІЛЕВСЬКИЙ