Силабус освітнього компонента
Програма навчальної дисципліни

Вступ до спеціальності. Ознайомча 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 дисципліни
Спеціальна (фахова),Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
1

Мова викладання
Українська, англійська

Викладачі, розробники

Гаврилова Алла Андріївна

alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації», «Безпека в DevOps», «Організація та безпека баз даних», «Управління IT-проєктами та їх безпека» у студентів бакалавріату
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Вступ до спеціальності. Ознайомча практика" є нормативною навчальною дисципліною. Дисципліна спрямована на підвищення рівня формування у студентів загального уявлення про теоретичну та практичну підготовку з основних послуг, механізмів та методів кібербезпеки, засобів захисту даних в глобальних та локальних комп'ютерних мережах, алгоритмів криптографічного та стеганографічного захисту даних; надання знання про особливості розробки та впровадження засобів захисту у комп'ютерній системі, отримання практичних навичок реалізації відомих алгоритмів захисту даних.

Мета та цілі дисципліни

Отримання студентами необхідних знань щодо особливостей становлення фахівців з питань кібербезпеки та захисту інформації.

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль –диференційований залік.

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК8. 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.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., практичні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Інформатика за шкільною програмою, Математика за шкільною програмою.

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, практичні заняття, співбесіда, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Кібербезпека – професія сьогодення та майбутнього. Початкові визначення спеціальності. Як стати спеціалістом з кібербезпеки. Як обрати спеціалізацію. Вимоги до фахівця з кібербезпеки. Як стати фахівцем з кібербезпеки.	2
Тема 2. Інститути, що забезпечують кіберзахист держави. Ситуаційний центр забезпечення кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України. Центр антивірусного захисту інформації держспецзв'язку України. Положення про організацію кіберзахисту за сферами діяльності України. CERT-UA. Нормативно-правова база. Визначення стану захищеності кіберпростору.	2
Тема 3. Напрямки захисту інформації. Методологічні основи кібербезпеки. Правове забезпечення інформаційної безпеки. Організаційний напрямок захисту інформації. Технічні (апаратні) заходи і засоби захисту інформації. Фізичні методи і засоби захисту. Програмно-технічні (програмно-апаратні) заходи захисту.	2
Тема 4. Загрози безпеки інформаційних систем. Класифікація загроз. Модель загроз інформаційної безпеки. Модель порушника. Можливі способи протидії загрозам.	4
Тема 5. Комп'ютерні злочини. Класифікація комп'ютерних злочинів. Комп'ютерні злочинці. Об'єкти комп'ютерних злочинів. Нормативна база.	2
Тема 6. Шифрування інформації. Практична реалізація шифру підстановки. Практична реалізація перестановочного шифру з ключовим словом. Практична реалізація перестановочного шифру з подвійним ключем.	4
Загальна кількість годин	**16**

Практичні заняття

Теми практичних/семінарських занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Корпоративні дані. Порівняння даних за допомогою гешу. 1. Типи корпоративних даних 2. Традиційні дані 3. Інтернет речей (IoT) та великі дані 4. Куб кіберзахисту	2	1
Тема 2.Наслідки порушення безпеки	1	0,5

1. Репутаційна шкода 2. Вандалізм 3. Крадіжка 4. Втрати доходу 5. Порушення прав інтелектуальної власності		
Тема 3. Захист пристроїв та мереж. **1. Захист** щодо убезпечення комп'ютерної техніки перед використанням 2. Безпека бездротової мережі для побутових користувачів 3. Ризики бездротових мереж	1	0,5
Тема 4. Створення та збереження надійних паролів. **1. Технологія захисту паролем** **2. Підходи щодо створення надійних паролей** **3. Парольна фраза** **4.** Правила вибору паролів 5. Перевірка пароля	2	1
Тема 5. Обслуговування даних. **1. Роль** шифрування для забезпечення безпеки даних 2. Алгоритм **шифрування даних за допомогою EFS у всіх версіях Windows**	2	1
Тема 6. Резервне копіювання даних для зовнішнього сховища. **1.** Резервне копіювання для запобігання втрати унікальних даних 2. Робота з кошиком видалення 3. Способи **гарантування видалення файлів безпечно і назавжди**	2	1
Тема 7. Хто володіє вашими даними. **1.** Угода про умови надання послуг 2. Політика використання даних 3. Налаштування конфіденційності 4. Політика безпеки	2	1
Тема 8. Захист конфіденційності в Інтернеті. **1.** Двофакторна аутентифікація 2. Відкрита авторизація 3. Конфіденційність електронної пошти та веб-браузера	2	1
Тема 9. Захист організації **1. Пристрої безпеки** **2. Міжмережні екрани** **3. Сканування портів** **4. Системи виявлення та запобігання вторгненням** **5. Виявлення в реальному часі** **6. Захист від шкідливого програмного забезпечення**	2	1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Оцінка ризиків поведінки в Інтернет	2

1. Інформація, якою безпечно ділитися в соціальних мережах 2. Небезпечні публікації у соцмережах 3. Менеджер паролів: як працює і чому корисний 4. Ризики, які виникають при завантаженні пробної версії програми 5. Ризики програм діагностики 6. Визначення небезпечності листів електронної пошти	
Тема 2. Визначення категорій міжмережних екранів	1
Загалом	$\sum_{i=1}^{m} b_i=3$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу.

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Різниця між ідентичністю офлайн та онлайн 1. Онлайн ідентичність 2. Отримання хакерами особистих даних 3. Визначення місцярозташування особистих даних 4. Способи інвестування у довгострокову вигоду від крадіжки особистих даних 5. Способи **реалізації несанкціонованої зацікавленості ідентичністю в Інтернеті** 6. Способи виявлення фішингових листів 7. Наслідки порушення безпеки даних	10
Тема 2. Сценарії порушення безпеки 1. Оримання хакеамри доступу до паролів облікових записів або фінансової інформації. **2. Загроза платформам електронного навчання** 3. Використання експлойтів для отримання доступу до цінної особистої інформації 4. Заходи для запобігання порушенням безпеки	8
Тема 3. Визначення сили паролю 1. Варіанти оновлення паролів мережі	8
Тема 4. Конфіденційність в Інтернеті 1. Обмін в соціальних мереж 2. Небезпека підроблених або фальсифікованих електронних листів 3. Режим приватного перегляду	8
Тема 5. Підхід до кібербезпеки на основі поведінки 1. Безпека на основі аналізу поведінки 2. NetFlow 3. Тестування на проникнення 4. Зменшення наслідків 5. Управління ризиками	8
Тема 6. Підхід Cisco до кібербезпеки **1.** Група Cisco CSIRT 2. Посібник з безпеки 3. Інструменти для запобігання та виявлення інцидентів 4. Cisco ISE та TrustSec	8

Тема 7. Правові та етичні питання **1.** Правові питання кібербезпеки 2. Етичні питання кібербезпеки 3. Питання корпоративної етики 4. Професійні сертифікації 5. Кар'єрні шляхи в галузі кібербезпеки	8
Загальна кількість годин	**58**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс «Введення в кібербезпеку» https://www.netacad.com/launch?id=da566b1e-9c68-4415-9144-17db9f04f43a&tab=curriculum&view=1341b26b-0c77-51c7-af8f-bdc7b0649c3e2.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Edited by Serhii Yevseiev, Volodymir 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. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. DOI: 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 Yerhidzei, Serhii Mykus, Yurii Pribyliev, Olena Akhiiezer, Mykhailo Shyshkin, Ivan Opirskyy, 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.

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/

3. Гаврилова Алла, Євсеєв Сергій. Аналіз стану захищеності блокчейн-проектів на ринку українських сервісів. Матеріали статей міжнародної науково-практичної конференції “Інтелектуальні системи та інформаційні технології”, Одеса, 2019. С. 62-64. URL: https://repository.kpi.kharkov.ua/bitstreams/cc4585ef-b64c-4a13-9afb-908754ac3d30/download
4. Гаврилова А.А., Королев Р.В. Анализ уязвимостей технологии блокчейн при работе с криптовалютами. Матеріали II Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”, Кропивницький, 2020. С. 4. https://kbpz.kntu.kr.ua/file/content/6635/2020-ii-mizhnarodna-naukovo-praktychnoi-konferentsiia-informatsiina-bezpeka-ta-informatsiini-tekhnolohii-.pdf
5. Гаврилова А.А. Аналіз криптографічних алгоритмів поданих до третього туру конкурсу NIST. Матеріали всеукраїнського круглого столу “Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони”, Харків, 2021. С. 361-365. URL:http://repository.hneu.edu.ua/handle/123456789/25621
6. Куля Ю.Е., Гаврилова А.А. Аналіз шифрів у бездротових мережах. Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених аспірантів та студентів “Стан, досягнення та перспективи інформаційних систем і технологій”, Одеса, 2021. С. 40-41. URL://http:Stan_dosyagnennya_inform_system_2021.pdf.
7. Гаврилова А.А. Визначення стану захищеності кіберпростору. Матеріали статей Міжнародної науково-практичної конференції “Інформаційні технології та комп’ютерне моделювання”, Івано-Франківськ, 2021. С. 11-12. URL:https://itcm.comp-sc.if.ua/2021 /zbirnyk_2021.pdf

Інформаційні ресурси

1. Havrylova Alla, Tkachov Andrii, Rahimova Irada Rahim Qizi. Estimating the Efficiency of Using the Modified UMAC Algorithm. 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, 2022. URL: https://ieeexplore.ieee.org/document/9916425/metrics#metrics

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,6	0,4		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: *П* – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
К – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$К = \frac{К_1 \cdot b_1 + К_2 \cdot b_2 + ... + К_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, *К*, *І*,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої *О* з округленням до найближчого цілого числа в більшу сторону.

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 політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, 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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Сергій ЄВСЕЄВ