Силабус освітнього компонента
Програма навчальної дисципліни

Вступ до спеціальності. Ознайомча практика

Шифр та назва спеціальності
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

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

Освітня програма
Національна безпека у сфері кіберзахисту

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
1

Мова викладання
Українська

Викладачі, розробники

ГАВРИЛОВА 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: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації» у студентів бакалавріата
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, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ–2. 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.
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до адаптації та дії в новій ситуації.
КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
КЗ–9. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
ФК–2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ФК–3. Здатність використовувати знання щодо ролі, місця та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконанні обов'язків з питань забезпечення національної безпеки.
ФК–5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.
ФК–9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.
ФК–13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку.

Результати навчання

ПРН–1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ПРН–2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
ПРН–3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН–4. Вільно спілкуватися державною мовою.
ПРН–5. Вільно спілкуватися іноземною мовою в межах потреби своєї професійної діяльності.
ПРН–6. Вміти адаптовуватись до нових викликів та дій у певних ситуаціях.
ПРН–7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
ПРН–8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.
ПРН–9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН–10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ПРН–11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки.
ПРН–12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
ПРН–13. Вміти використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.
ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
ПРН–17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
ПРН–19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.
ПРН–21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні 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

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

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.
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.
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.
Тема 4. Загрози безпеки інформаційних систем.

Класифікація загроз. Модель загроз інформаційної безпеки. Модель порушника. Можливі способи протидії загрозам.
Тема 5. Комп'ютерні злочини.
Класифікація комп'ютерних злочинів. Комп'ютерні злочинці. Об'єкти комп'ютерних злочинів. Нормативна база.
Тема 6. Шифрування інформації.
Практична реалізація шифру підстановки. Практична реалізація перестановочного шифру з ключовим словом. Практична реалізація перестановочного шифру з подвійним ключем. Практична реалізація шифру Цезаря. Практична реалізація шифру Цезаря з ключовим словом. Практична реалізація шифру дошки (квадрата) Полібія. Практична реалізація Афінного шифру. Практична реалізація шифру Віженера.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Корпоративні дані. Порівняння даних за допомогою гешу.
Тема 2. Наслідки порушення безпеки.
Тема 3. Захист пристроїв та мереж.
Тема 4. Створення та збереження надійних паролів.
Тема 5. Обслуговування даних.
Тема 6. Резервне копіювання даних для зовнішнього сховища.
Тема 7. Хто володіє вашими даними.
Тема 8. Захист конфіденційності в Інтернеті.
Тема 9. Дослідження ризиків своєї поведінки в Інтернеті

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
Intr to Cyber, Getting Started with Cisco Packet Tracer
https://www.netacad.com/catalogs/learn?category=course

Література та навчальні матеріали

Основна література:

1. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

3. 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
4. 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.

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 Journal. 2023, Vol. 25, №. 1. P. 6-19.
https://jrnl.nau.edu.ua/index.php/ZI/article/view/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.
https://www.researchgate.net/publication/372148604_Development_of_an_improved_SSLTLS_protocol_using_post-quantum_algorithms/fulltext/64a8b0e6c41fb852dd5b9156/Development-of-an-improved-SSL-TLS-protocol-using-post-quantum-algorithms.pdf
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.
4. 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.
https://ice.nure.ua/ua/student-publications/2021/
5. 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.
https://ice.nure.ua/ua/student-publications/2021/
6. 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.
https://www.researchgate.net/profile/Vasyl-Gorbachuk/publication/368636872_Modern_cloud_concepts_technologies_applications_services_and_platforms/links/63f14d032958d64a5cde853a/Modern-cloud-concepts-technologies-applications-services-and-platforms.pdf
7. 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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП
Андрій ТКАЧОВ