НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-46S

СИЛАБУС *навчальної дисципліни*		**SYLLABUS**
Кібербезпека інформаційних систем		Cyber security of information systems
Шифр за ОП	ПП-4	Code in Degree Programme
Освітній рівень: Магістрський (другий)		Level of Education: Master's (second)
Галузь знань Інформаційні технології	12	Field of Knowledge Information Technology
Спеціальність Інформаційні системи та технології	126	Field of Study Information systems and technology
Освітня програма: Інформаційні технології в бізнесі		Degree Programme: Information technologies in business

РІВНЕ – 2024

Силабус навчальної дисципліни «Кібербезпека інформаційних систем» для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою «Інформаційні технології в бізнесі», спеціальності «Інформаційні системи та технології»,Рівне. НУВГП. 2024. 10 стор.

ОП на сайті університету:

Освітньо-професійна програма "Інформаційні технології в бізнесі" | (nuwm.edu.ua)

Розробник силабусу: Бабич С.В., к.т.н., старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри
Протокол № 11 від “14” травня 2024 року

Завідувач кафедри: в.о. СидорА.І., к. т. н., доцент, кафедри обчислювальної техніки

Керівник (гарант) ОП: Барановський С.В., кандидат технічних наук, доцент, доцент кафедри комп’ютерних технологій та економічної кібернетики

Схвалено науково-методичною радою з якості ННІ
Протокол № 7 від “ 17 ” червня 2024 року

Голова науково-методичної ради з якості ННІ: Мартинюк П.М., д.т.н., професор

Попередня версія силабусу: відсутня.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Кібербезпека інформаційних систем»	
ОК «Кібербезпека інформаційних систем» є складовою ОП, спрямована на досягнення визначених результатів навчання, якій встановлено форму підсумкового контролю та визначено кількість кредитів ЄКТС.	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*Магістр*
Освітня програма	*Інформаційні технології в бізнесі*
Спеціальність	*Інформаційні технології*
Рік навчання, семестр	*1* *2*
Кількість кредитів	*4*

Лекції:	*18 години*
Лабораторні заняття:	*22 години*
Самостійна робота:	*80 годин*
Курсова робота:	*ні*
Форма навчання	*денна*
Форма підсумкового контролю	*екзамен*
Мова викладання	*українська*
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА	
Лектор	*Бабич Сергій Васильович, к.т.н., ст. викладач кафедри обчислювальної техніки*
ORCID	*http://orcid.org/ 0000-0002-8669-7288*
Як комунікувати	*s.v.babych@nuwm.edu.ua* *тел. 093-772-13-61*
ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ	
Мета та завдання	

Метою викладання дисципліни: "Кібербезпека інформаційних систем" є:

– отримання здобувачами вищої освіти теоретичних знань та практичних навичок побудови захищених інформаційних систем на основі сучасних засобів технічного та криптографічного захисту інформації;

– формування системного підходу до побудови захищених інформаційних систем;

– набуття навиків блокування технічних каналів витоку інформації;

– отримання знань порядку застосування методів захисту від несанкціонованого доступу;

– сформувати знання, вміння і навички, необхідні для самостійного аналізу інформаційних систем в сфері безпекових питань, розвинути здатність до самостійного вивчення навчальної літератури.

Навчальний курс призначений для вивчення основних засобів та заходів захисту інформації в інформаційних системах, в якому класифіковано загрози для інформації за критеріями цілісності, конфіденційності та доступності, методів та засобів їх локалізації та блокування. Подано основні принципи формування систем технічного та криптографічного захисту інформації. Надано описи та розглянуто принципи дії сучасних криптоалгоритмів, засобів хешування, генерації та технологій електронного цифрового підпису.

Посилання на розміщення освітнього компонента на навчальній платформі Moodle, на платформі освітніх програм та їхніх освітніх компонентів

Курс: Кібербезпека інформаційних систем | (nuwm.edu.ua)

Передумови вивчення
(місце освітнього компоненту в структурно-логічній схемі)

Для вивчення даного курсу студентам необхідні знання з такої дисципліни – ЗП-3 «Нереляційні бази даних».

На матеріалі даної дисципліни ґрунтується вивчення наступних професійно спрямованих дисциплін: ПП-5 «Науково-дослідницька практика», ПП-6 «Кваліфікаційна робота магістра».

Компетентності

ЗК02. Здатність спілкуватися іноземною мовою.

ЗК03. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань та видів економічної діяльності).

СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

СК07. Розробляти і реалізовувати інноваційні проекти у сфері інформаційних систем.

СК08. Здатність до інформаційної підтримки діяльності підприємств водогосподарського комплексу та комп'ютерного моніторингу систем природокористування.

Програмні результати навчання (ПРН)

РН02. Вільно спілкуватись державною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності.

РН04. Управляти процесами розробки, впровадження та експлуатації у сфері ІСТ, які є складними, непередбачуваними і потребують нових стратегічних та командних підходів.

РН07. Здійснювати обґрунтований вибір проектних рішень та проектувати сервіс-орієнтовану інформаційну архітектуру підприємства (установи, організації тощо).

РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

РН12. Формувати вимоги, створювати концепцію, проектувати, розробляти та супроводжувати інформаційні системи підтримки функціонування підприємств водогосподарського комплексу.

Структура та зміст освітнього компонента

Тема 1. Моделі загроз інформації та порушника безпеки ІС.

Результати навчання– РН02.

Опис теми. Механізми та сервіси захисту ІС. Головні завдання безпеки ІС. Модель порушника безпеки інформаційної системи. Механізми та сервіси упередження. Класифікація атак на інформацію та інформаційну систему.Головні завдання безпеки ІС.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 1. Характеристика каналів витоку інформації.

Тема 2. Традиційні криптосистеми. Симетричні криптосистеми.

Результати навчання– РН02, РН04, РН10.

Опис теми. Криптографічні методи та засоби захисту інформації. Аналітичне представлення обстановки. Класифікація каналів витоку інформації. Середовище поширення і спосіб перехвату.

Лекція – 2 год.

Лабораторна робота – 4 год.

Лабораторна робота № 2. Дослідження можливостей Bouncy Castle Crypto package.

Тема 3. Криптографія з відкритим ключем. Асиметричні криптосистеми.

Результати навчання– РН02, РН04, РН07.

Опис теми. Заходові методи. Беззаходові методи. Організаційний захист. Заходи безпеки. Служба безпеки. Системи контролю доступу.Класифікація цифрових підписів. Механізми аутентифікації у стеку TCP/IP. Механізми аутентифікації у стеку PSEC. Схеми проходження IP-пакету даних в транспортному режимі. Безпека програм та даних.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 3. Система управління інформаційною безпекою

Тема 4. Моделі інформаційних систем.

Результати навчання– РН04, РН10.

Опис теми. Дискреційне розмеження доступу. Моделі на основі матриці доступу. Моделі поширення прав доступу. Концепція побудування синергетичної моделі загроз безпеки банківських інформаційних ресурсів.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 4. Проведення моніторингу та аналізу ризиків.

Тема 5. Загрози та вразливості. Використання IDS та IPS.

Результати навчання– РН04, РН07.

Опис теми. Вразливості IP. Атаки на основі ARP. Вразливості TCP та UDP. Атаки на те, що ми робимо. Корпоративні сервіси. Класифікатор загроз. Оцінювання сповіщень Security Onion. Способи моніторингу системи. Інструменти аналізу. Генерація сповіщень. Способи моніторингу системи.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 5. Аналіз загроз для інформаційних систем. Призначення, наслідки, протидія.

Тема 6. Системи активного захисту.

Результати навчання– РН04, РН07, РН12.

Опис теми. Технологія «Горщик з медом» (honeycomb) та інформаційні системи активного мережевого захисту. Створення фейкової інфраструктури мережі та ІСТ. Приманки. Деанонімізація зловмисника. Вплив загроз. Сучасний центр моніторингу та управління безпекою (SOC).

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 6. Побудова EDZ – зони мережі та створення пасток в межах активного мережевого захисту.

Тема 7. Управління безпечною мережею.

Результати навчання– РН04, РН07, РН12

Опис теми. Політика інформаційної безпеки. Політики резервного копіювання даних. Класифікатор мережевих загроз. Удосконалена модель інфраструктури АБС. Моделі мережевої безпеки. Координація дій різних агентів під час кризової Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 7. Огляд можливостей та імплементації систем візуалізації та управління подіями (SIEM).

Тема 8. Управління кіберінцидентами.

Результати навчання– РН02, РН07, РН10.

Опис теми. Ключові критерії для класифікації кіберінцидентів від легких до складних. Кіберінциденти мережевого характеру. Вразливості IP. Атаки на основі ICMP. Атаки за методом підсилення та відбиття. Атаки з підміною адрес. Вразливості TCP та UDP. Атаки на те, що ми робимо. Корпоративні сервіси. Класифікатор загроз.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 8. Виявлення, ідентифікація, аналіз та реагування на інциденти інформаційної та/або кібербезпеки..

Тема 9. Деструктивні методи соціальної інженерії.

Результати навчання– РН02, РН04, РН07.

Опис теми. Захист від деструктивних методів соціальної інженерії. Вторгнення і заходи протидії. Фішинг (цільовий фішинг). Зворотна соціальна інженерія. Методи маніпуляції людьми.

Лекція – 1 год.

Лабораторна робота – 2 год.

Лабораторна робота № 9. Соціальна інженерія. Вивчення інструментів для аудиту безпеки і проведення атак.

Тема 10. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.

Результати навчання– РН02, РН10, РН12.

Опис теми. Digital Security. Збереження даних у платіжній інфраструктурі. Виявлення загроз у платіжній інфраструктурі. Управління кіберризиком. Вибір методів та засобів забезпечення необхідного рівня ІБ.

Лекція – 1 год.

Лабораторна робота – 2 год.

Лабораторна робота № 10. Проведення аудиту інформаційної безпеки на базі аудиту мережі.

Форми та методи навчання

Використовуються такі методи навчання: лекційні заняття проводяться з використанням проектора для демонстрації процесу дослідження стійкості інформаційних систем та програмного забезпечення, зокрема при архітектури «файл–сервер» та «клієнт–сервер».

Тематика лабораторних робіт розрахована, у тому числі, й на виконання завдань учбово-дослідного характеру з частково невизначеними умовами.

Програма освітньої компоненти передбачає комплексне навчання вивчення засобів та заходів захисту інформаційних систем в усіх її аспектах з формуванням визначених в освітній програмі фахових компетентностей магістра з інформаційних технологій в бізнесі.

Інструменти, обладнання, програмне забезпечення

Курс передбачає вивчення загальних характеристик і можливостей сучасних CASE – засобів, як програмних інструментів підтримки проектування та використання безпекових рішень в інформаційних системах.

Порядок оцінювання програмних результатів навчання/ результатів навчання

Для поточного контролю знань студентів з навчальної дисципліни використовуються такі методи:

-на лекційних заняттях проводиться контроль присутності студентів та контроль якості конспектів лекцій;

-на лабораторних заняттях проводиться контроль готовності до заняття шляхом тестового експрес-опитування, а також шляхом захисту звітів з лабораторної роботи у вигляді співбесіди;

-контроль самостійної роботи проводиться у вигляді співбесіди на задану тему;

-оцінка модульних контрольних робіт (тестування);

Підсумковий контроль проводиться в кінці семестру у вигляді екзамену.

Усі форми контролю включено до 100-бальної шкали оцінювання.

Оцінювання результатів поточної роботи (завдань, що виконуються на лабораторних заняттях, результати самостійної роботи студентів) проводиться за такими критеріями:

Лабораторні роботи (у балах, виділених на завдання із заокругленням до цілого числа):

0 балів – завдання не виконано;

2 бали – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру;

3 бали – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці;

4 бали – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

5 балів – завдання виконано правильно, вчасно і без зауважень.

Модульний контрольпроходитиме у формі тестування. У тесті 30 запитань різної складності: рівень 1 – 24 запитань по 0,5 бали (12 балів), рівень 2 – 2 запитань по 2 бали (4 бали), рівень 3 – 1 запитання по 4 бали (4 бали). Усього – 20 балів.

Допуск до екзамену:

-усі лабораторні роботи відроблені;

-виконання двох модульних контрольних робіт;

Результати поточного контролю у першому семестрі оцінюються за шкалою [0...60] балів. За підсумковий контроль у вигляді екзамену, студент може отримати [0...40] балів. У такому випадку до набраних під час екзамену балів додаються бали поточного контролю.

Нормативні документи: Навчально-науковий центр незалежного оцінювання | (nuwm.edu.ua).

Рекомендована література (основна, допоміжна)

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.
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.
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.

Допоміжна література.

1. URL: ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model.
2. URL: ISO/IEC WD 15408-2 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components.
3. URL: ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

Інформаційні ресурси в Інтернет

1. URL: Національна бібліотека України імені В. І. Вернадського (nbuv.gov.ua)
2. URL: Рівненська обласна універсальна наукова бібліотека (libr.rv.ua)
3. URL: Рівненська централізована бібліотечна система (rivnecbs.com.ua)
4. URL: Бібліотека НУВГП (nuwm.edu.ua)

Поєднання навчання та досліджень

Студенти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, а також можуть бути долучені до написання та опублікування наукових статей з тематики курсу.

Кожен здобувач вищої освіти може залучатися до написання та реалізації наукових робіт, статей, тез, патентів, проектів та інших робіт всеукраїнських та міжнародних досліджень.

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

Перелік соціальних, «м'яких» навичок (soft skills)

Здатність застосовувати знання у практичних ситуаціях.

Здатність спілкуватися державною мовою як усно, так і письмово

Здатність працювати в команді.

Дедлайни та перескладання

Ліквідація академічної заборгованості здійснюється згідно: Порядок ліквідації академічних заборгованостей у НУВГП | (nuwm.edu.ua). Згідно цього документу і реалізується право студента на повторне вивчення дисципліни чи повторне навчання на курсі.

Перездача модульних контролів здійснюється згідно з: Якість освіти | (nuwm.edu.ua).

Оголошення стосовно дедлайнів здачі та перездачі оприлюднюються на сторінці: MOODLE - НУВГП | (nuwm.edu.ua).

Неформальна та інформальна освіта (за потреби)

Здобувачі освіти мають право на перезарахування результатів навчання у неформальній та інформальній освіті не більше ніж 25% загальної кількості кредитів освітньої програми на семестр – Центр неформальної освіти | (nuwm.edu.ua).

Правила академічної доброчесності

За списування під час проведення модульного контролю чи підсумкового контролю, студент позбавляється подальшого права здавати матеріал і у нього виникає академічна заборгованість.

За списування під час виконання окремих завдань, студенту знижується оцінка у відповідності до ступеня порушення академічної доброчесності.

Документи стосовно академічної доброчесності (про плагіат, порядок здачі курсових робіт, кодекс честі студентів, документи Національного агентства стосовно доброчесності) наведені на сторінці ЯКІСТЬ ОСВІТИ сайту НУВГП – Академічна доброчесність | (nuwm.edu.ua).

Вимоги до відвідування

Санкції за пропуски пар не передбачені. Студент має можливість самостійно вивчити необхідний для здачі модульних контролів та лабораторних робіт матеріал, який в повному обсязі дублюється викладачем одночасно на платформі Moodle та/або у групі з даного предмету в месенджері Telegram.

У разі необхідності проведення консультації – викладач йде назустріч. Відвідування пари допускається із використанням власного ноутбука. Студенти не повинні порушувати дисципліну на парі. Для студентів, які знаходяться на індивідуальному плані навчання, надаються індивідуальні завдання.

Студент має право оформити індивідуальний графік навчання згідно з Положення про індивідуальний графік навчання студентів денної форми навчання Національного університету водного господарства та природокористування | (nuwm.edu.ua).

Автор
В.О. завідувача кафедри ОТ — Андрій СИДОР

Затверджено

Проректор з науково-педагогічної та навчальної роботи — Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №864
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100