НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-47S

СИЛАБУС *навчальної дисципліни*		**SYLLABUS**
Безпека інформаційних систем та захист інформації		Security of information systems and protection of information
Шифр за ОП	ОК-27	Code in Degree Programme
Освітній рівень: бакалаврський (перший)		Level of Education: Bachelor's (first)
Галузь знань Інформаційні технології	12	Field of Knowledge Information Technologies
Спеціальність Інформаційні системи та технології	126	Field of Study Information systems and technology
Освітня програма: Інформаційні системи і технології		Degree Programme: Information systems and technology

РІВНЕ – 2024

Силабус навчальної дисципліни «Безпека інформаційних систем та захист інформації» для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою «Інформаційні системи і технології», спеціальності «Інформаційні системи та технології»,Рівне. НУВГП. 2024. 10 стор.

ОП на сайті університету:

Освітньо-професійна програма «Інформаційні системи і технології» | (nuwm.edu.ua)

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

Силабус схвалений на засіданні кафедри
Протокол № 10 від “14” травня 2024 року

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

Керівник (гарант) ОП: Гладка Олена Миколаївна, к.т.н., 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: 04-05-25S

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ‹Безпека інформаційних систем та захист інформації›	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*Бакалавр*
Освітня програма	*Інформаційні системи і технології*
Спеціальність	*Інформаційні системи та технології*
Рік навчання, семестр	*3* *6*
Кількість кредитів	*4,5*
Лекції:	*24/2 години*
Лабораторні заняття:	*24/10 години*

Самостійна робота:	*87/123 годин*
Курсова робота:	*ні*
Форма навчання	*денна, заочна*
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 НАВЧАЛЬУ ДИСЦИПЛІНУ

Мета та завдання

Метою викладання дисципліни: "Безпека інформаційних систем та захист інформації" є отримання здобувачами компетентностей з: проводження аналізу загроз інформаційної безпеки, основними методами, принципами, алгоритмами захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників; отримання знань порядку застосування методів захисту від несанкціонованого доступу.

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: Безпека інформаційних систем та захист інформації | (nuwm.edu.ua)
Передумови вивчення (місце освітнього компоненту в структурно-логічній схемі)
Для вивчення даного курсу студентам необхідні знання з таких дисциплін – ОК-13 «Архітектура комп'ютерів», ОК-16 «Операційні системи та системне програмне забезпечення», ОК-25 «Комп'ютерні мережі». *На матеріалі даної дисципліни ґрунтується вивчення наступних професійно спрямованих дисциплін: ОК-17 «Веб-технології та веб-дизайн».*
Компетентності
КЗ08. Здатність оцінювати та забезпечувати якість виконуваних робіт. *КС06. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.* *КС08.Здатність управляти якістю продуктів і сервісів інформаційних систем та технологій протягом їх життєвого циклу.*
Програмні результати навчання (ПРН)
ПР03. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій. *ПР10. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.*
Структура та зміст освітнього компонента
Тема 1. Правові аспекти безпеки інформаційних систем. Результати навчання– ПР03, ПР10. Опис теми. Закон України "Про інформацію". Закон України "Про науково-технічну інформацію". Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Закон України "Про основні засади забезпечення кібербезпеки України". Закон України "Про державну таємницю". Закон України "Про захист персональних даних". Регламент європейського Парламенту і Ради. GENERAL DATA PROTECTION REGULATION. Інтеграція управління ризиком у життєвий цикл розвитку систем. Єдині критерії оцінки безпеки інформаційних технологій ISO/IEC 15408. Рамкова програма з кібербезпеки. Лекція – 2 год.

Лабораторна робота – 2 год.
Лабораторна робота № 1. Характеристика стандартів із забезпечення кібербезпеки.

Тема 2. Напрямки забезпечення безпеки інформаційних систем.
Результати навчання– ПР03, ПР10.
Опис теми. Канали несанкціонованого отримання даних. Напрямки забезпечення інформаційної безпеки. Організаційний захист. Системи контролю доступу. Правовий і технічний захист інформації. Аналіз ризиків.
Лекція – 2 год.
Лабораторна робота – 2 год.
Лабораторна робота № 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).

Тема 3. Способи захисту інформації.
Результати навчання– ПР03, ПР10.
Опис теми. Забезпечення інформаційної безпеки. Організаційні заходи. Організаційно-технічні заходи. Характеристика захисних дій. Система безпеки. Основні положення політики безпеки. Моделі секретних систем.
Лекція – 2 год.
Лабораторна робота – 2 год.
Лабораторна робота № 3. Дослідження заходів безпеки інформаційних систем.

Тема 4. Основні безпекові моделі інформаційних систем.
Результати навчання– ПР03, ПР10.
Опис теми. Основні моделі інформаційної безпеки. Моделі поширення прав доступу. Моделі безпеки на основі тематичної політики. Ієрархічна система ролів. Дводольна система робочих груп.
Лекція – 2 год.
Лабораторна робота – 2 год.
Лабораторна робота № 4. Вивчення та аналіз основних безпекових моделейінформаційних систем.

Тема 5. Внутрішні та зовнішні загрози. Ризики та інциденти.
Результати навчання– ПР03, ПР10.
Опис теми. Ключові критерії для класифікації кіберінцидентів від легких до складних. Атаки на основі ICMP. Атаки за методом підсилення та відбиття. Атаки з підміною адрес. Корпоративні сервіси. Класифікатор загроз. Системи виявлення/запобігання вторгнень. Способи моніторингу системи.
Лекція – 2 год.
Лабораторна робота – 2 год.
Лабораторна робота № 5. Аналіз загроз для інформаційних систем. Призначення, наслідки, протидія.

Тема 6. Фізичний захист об'єктів інформаційних систем.
Результати навчання– ПР03, ПР10.
Опис теми. Зламування особистих даних. Компанії, які стали жертвою шантажу. Країни, які зазнали нападу. Хакери Непрофесіонали. Хакери Хактивісти. Вплив загроз. Фізичний захист

об`єктів критичної інфраструктури. Захист інфраструктурних комунікацій.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 6. Розгляд заходів від внутрішніх та зовнішніх загроз. Використання IDS та IPS.

Тема 7. Управління кризовими ситуаціями та ліквідація наслідків.

Результати навчання– ПР03, ПР10.

Опис теми. Організація ефективного управління кризовими ситуаціями в критичній інфраструктурі. Класифікатор загроз. Моделі безпеки. Відновлення функціонування інформаційної системи після реалізації загроз, кібератак, збоїв та відмов різних класів та походження.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 7. Здійснювати обґрунтований вибір проектних рішень та проектувати сервіс-орієнтовану інформаційну архітектуру підприємства (установи, організації тощо).

Тема 8. Класифікація кіберінцидентів.

Результати навчання– ПР03, ПР10.

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 – 4 год.

Лабораторна робота – 2 год.

Лабораторна робота № 8. Дослідження стійкості захисту інформаційних систем.

Тема 9. Основи соціальної інженерії в безпеці ІС та захисту інформації.

Результати навчання– ПР03.

Опис теми. Сутність соціальної інженерії. Розуміння поведінки людей. Розробка стратегій впливу. Виявлення вразливостей. Підходи до визначення сутності соціальної інженерії.

Лекція – 4 год.

Лабораторна робота – 4 год.

Лабораторна робота № 9. Соціальна інженерія. Вивчення мережевих атак.

Тема 10. Інструментальні засоби управління ризиками інформаційної безпеки.

Результати навчання– ПР03, ПР10.

Опис теми. Моделі оцінки ризиків компанії. Digital Security. Модель аналізу загроз та вразливостей. Модель аналізу загроз та вразливостей. Завдання контрзаходів. Зниження часу відновлення функціонування. Розслідування кіберінцидентів / кібератак.

Лекція – 2 год.

Лабораторна робота – 4 год.

Лабораторна робота № 10. Дослідження та аналіз основних моделей загроз та вразливостей інформаційних систем.

Форми та методи навчання
Використовуються такі форми навчання: самостійна робота студентів, лабораторні заняття, лекційні заняття, що проводяться з використанням проектора для демонстрації процесу дослідження стійкості інформаційних систем та програмного забезпечення. *Тематика лабораторних робіт розрахована, у тому числі, й на виконання завдань навчально-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 бакалавра з інформаційних систем та технологій.*
Інструменти, обладнання, програмне забезпечення
Курс передбачає використання: консольних команд середовища windwows та unix/linux; програм: honeycomb software, SIEM software, wireshark; а також засобів моделювання середовища: Networking Simulation Tool Cisco Packet Tracer - Networking Simulation Tool, virtual box (wmware).
Порядок оцінювання програмних результатів навчання/ результатів навчання

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

-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 контроль проходитиме у формі тестування. У тесті 27 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 семестрового контролю 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. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

2. М.В. Захарченко, В.Г. Кононович, В.И. Кільдішев, Д.В. Голев. «Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД.». - 2011.

3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. Часопис Київського університету права. 2018. № 3. С. 235–239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54

2. Білявська Ю., Микитенко Н, Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. Товари і ринки. 2021. №1. С. 34–46. URL: http://nbuv.gov.ua/UJRN/tovary_2021_1_5

3. Бойко В. Д., Василенко М. Д., Кухаренко С. В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. Інформаційна безпека людини, суспільства, держави. 2019. №3. С. 57–69. URL: http://nbuv.gov.ua/UJRN/iblsd_2019_3_8

4. Бурячок В. Л. Інформаційна та кібезбезпека: соціотехнічний аспект. Львів : Магнолія – 2006, 2018. 320 с.

5. Горлинський В., Горлинський Б. Кібербезпека як складова інформаційної безпеки України. Information Technology and Security. 2019. Vol. 7, Iss. 2. С. 136–148. URL: http://nbuv.gov.ua/UJRN/inftech_2019_7_2_5

6. Даник Ю. Г. Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Вид. 2-ге, перероб. та доп. Одеса.: ОНАЗ ім. О. С. Попова, 2019. 320 с.

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

4. Хорошко В. А. Методи та засоби захисту інформації. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.

5. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.

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.

Формування та розвиток критичного та аналітичного мислення.

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 №844
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100