НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-36S

СИЛАБУС *навчальної дисципліни*		**SYLLABUS**
Захист інформації в комп'ютерних системах		Computer systems information security
Шифр за ОП	**ОК 32**	Code in Degree Programme
Освітній рівень: Бакалаврський (перший)		Level of Education: Bachelor's (first)
Галузь знань **Інформаційні технології**	**12**	Field of Knowledge **Information Technology**
Спеціальність **Комп'ютерна інженерія**	**123**	Field of Study **Computer Engineering**
Освітня програма: **Комп'ютерна інженерія**		Degree Programme: **Computer Engineering**

РІВНЕ – 2024

Силабус навчальної дисципліни «Захист інформації в комп'ютерних системах» для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою *«Комп'ютерна інженерія», спеціальності «Комп'ютерна інженерія», 123*. Рівне. НУВГП. 2024. 16 стор.

ОП на сайті університету: https://ep3.nuwm.edu.ua/22990/

Розробники силабусу: *Шатна Анастасія Володимирівна, старший викладач кафедри обчислювальної техніки;*
Шатний Сергій В'ячеславович, к.т.н., доцент кафедри обчислювальної техніки;
Багнюк Ольга Миколаївна, старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри обчислювальної техніки
Протокол № 8 від 22.03.2024 року

Завідувач кафедри: *Круліковський Б.Б., к.т.н., доцент*.

Керівник (гарант) ОП: *Сидор А.І., к.т.н., доцент*.

Схвалено науково-методичною радою з якості ННІ КІТІ
Протокол № від 6 від 8.04.2024 року

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

Попередня версія силабусу: відсутня.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	
Захист інформації в комп'ютерних системах	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*Бакалавр*
Освітня програма	*Комп'ютерна інженерія*
Спеціальність	*123 Комп'ютерна інженерія*
Рік навчання, семестр	*3-й рік, 2-й семестр*
Кількість кредитів	*5*
Лекції:	*24/4 години*
Лабораторні заняття:	*26/12 годин*
Самостійна робота:	*100/134 годин*

Курсова робота:	*Ні*
Форма навчання	*денна/заочна*
Форма підсумкового контролю	*Іспит*
Мова викладання	*Державна*
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА	
Лектор 	*Шатний Сергій В'ячеславович* *к.т.н., доцент кафедри обчислювальної техніки*
Вікіситет	*https://wiki.nuwm.edu.ua/index.php/Шатний_Сергій_В%27ячеславович*
ORCID	*https://orcid.org/0000-0003-4650-5090*
Канали комунікації	*s.v.shatnyi@nuwm.edu.ua*
Асистент лектора 	*Шатна Анастасія Володимирівна* *старший викладач кафедри обчислювальної техніки*
Вікіситет	http://wiki.nuwm.edu.ua/index.php/Шатна_Анастасія_Володимирівна
ORCID	https://orcid.org/ 0009-0006-2499-8591
Канали комунікації	*a.v.shatna@nuwm.edu.ua*

Асистент лектора 	*Багнюк Ольга Миколаївна* *старший викладач кафедри обчислювальної техніки*
Вікіситет	https://wiki.nuwm.edu.ua/index.php/Багнюк_Ольга_Миколаївна
ORCID	https://orcid.org/0000-0002-7898-2337
Канали комунікації	o.m.bahniuk@nuwm.edu.ua

ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Мета та завдання

Метою обов'язкової дисципліни є формування у студентів базових понять та знань теорії, принципів побудови, стандартів, алгоритмів функціонування сучасних захищених комп'ютерних мереж, знань базових підходів до побудови, технологій, протоколів, обладнання, програмного забезпечення в сфері захисту комп'ютерних систем та мереж.

Опанування дисципліни спрямовано на формування у студентів професійних компетентностей, отриманню знань щодо існуючих технологій та програмно-апаратних засобів захисту комп'ютерних мереж, базових теоретичних та практичних аспектів організації засобів захисту інформації, а також сприяє отриманню необхідних навичок з практичного використання засобів захисту інформації, включаючи використання різних можливостей обмеження доступу до захищених ресурсів.

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

https://exam.nuwm.edu.ua/course/view.php?id=2718

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

Дисципліни, що передують вивченню: ОК28 Комп'ютерні системи і мережі.

Отримані навички можуть використовуватись при подальшому вивченні дисциплін: ВБ 5.2. Криптографічний захист інформації, ВБ 4.2. Технічне забезпечення інформаційної безпеки та ВБ 5.1. Паралельні та розподілені обчислення

Компетентності
Р1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії. *Р4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.* *Р8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.* *Р12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.*
Програмні результати навчання (ПРН). Результати навчання (РН)*
N1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж. *N6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.* *N7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.* *N8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.* *N9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.* *N11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії* *N13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.* *N23. Здатність адаптуватись до нових ситуацій, обґрунтувати, приймати та реалізовувати у межах компетенції рішення.* *N24. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.*

СТРУКТУРА ТА ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Теми (лекції)	Опис лекції	№	Теми лабораторних занять
МОДУЛЬ 1. БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ				

1	Технології захисту інформації в комп'ютерних системах (2 год.) *N1, N11*	Інформаційна безпека. Історія інформаційної безпеки . Базова тріада інформаційної безпеки CIA-triad [ЦРУ, 1980]. Властивості інформації, що підлягають захисту.	1	Класичні методи шифрування. Шифр Цезаря. (2 год.)
2	Нормативно-правовий захист інформації (2 год.) *N6, N23*	Нормативно-правовий захист інформації . Нормативна база інформаційної безпеки. Закони України про захист інформації.	2	Моноалфавітний шифр. Шифр Плейфера. (2 год.)
3	Розроблення захищених ОС (2 год.) *N9, N13*	Поняття захищеної операційної системи. Підходи до побудови захищених операційних систем. Порівняння підходів до побудови захищених операційних систем.	3	Шифрування та дешифрування шифру Хілла. (4 год.)
4	Програмні засоби захисту інформації. Параметри безпеки Linux та інших операційних систем. (2 год.) *N7, N9*	Особливості архітектури Linux. Забезпечення безпеки в Linux.		

5	Спеціалізовані комплекси засобів захисту ПЕОМ. (2 год.) *N8, N13*	Основні положення. Функції, які реалізують спеціалізовані КЗЗ. Функціональний профіль захищеності і рівень гарантій. Політика функціональних послуг безпеки. Описи реалізованих функцій.	4	Багатоалфавітні шифри. Шифр транспозиції. (4 год.)
6	Симетричні криптоалгоритми. Мережа Фейстеля. Криптоалгоритм DES. (2 год.) *N24, N1*	Вимоги до блокового алгоритму шифрування. Мережа Фейстеля. Криптоалгоритм DES.		
МОДУЛЬ 2. СИСТЕМА АНАЛІЗУ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ				
7	Алгоритм Діффі-Хеллмана. Асиметричний криптоалгоритм RSA. (2 год.) *N6, N7*	Основні відомості. Шифрування та розшифрування. Приклади обчислень. Практичне використання.	5	Робота врежимі блокового шифру. Стандарт шифрування DES. (4 год.)
8	ХЕШ-функція. Електронний цифровий підпис. Акредитовані центри сертифікації ключів. (2 год.) *N9, N13*	Основні відомості. Застосування хеш-функцій. Сучасні алгоритми хешування. Електронний цифровий підпис.	6	Шифрування та дешифрування методом Фейстеля (2 год.)

9	Створення комплексної системи захисту інформації (частина 1) (2 год.) *N7, N9*	Загальні вимоги щодо створення комплексної системи захисту інформації. Структура комплексної системи захисту інформації. Створення комплексної системи захисту інформації. Вимоги до комплексної системи захисту інформації та політика безпеки.		
10	Створення комплексної системи захисту інформації (частина 2). (2 год.) *N1, N11*	Розроблення політики безпеки. Концепція безпеки інформації в АС. Аналіз ризиків. Визначення вимог до заходів, методів і засобів захисту.	7	Розширений стандарт шифрування AES. (4 год.)
11	Криптографічний захист інформації. (2 год.) *N6, N24*	Криптографічна система захисту інформації. Блокове шифрування . Шифри перестановки.	8	Розширений стандарт дешифрування AES. (4 год.)
12	Електронна система документообігу. Електронні ключі. (2 год.) *N8, N11*	Сфери поширення електронного документообігу. Облікова система електронного документообігу. Використання алгоритмів асиметричного шифрування при реалізації електронного цифрового підпису.		

Форми, методи та технології навчання

Форми навчання	• *очна (денна) з, можливо, елементами дистанційного навчання;* • *заочна.*
Форми навчального процесу	• *навчальні заняття (лекції, лабораторні заняття, консультації);* • *самостійна робота здобувачів;* • *робота в наукових бібліотеках та мережі Інтернет;* • *контрольні заходи (поточна складова оцінювання, модульні контролі, підсумковий контроль).*
Методи та технології навчання	• *робота в малих групах (команді) та індивідуальна робота;* • *проектна технологія;* • *аналіз конкретних ситуацій (case study): ситуація-оцінка;* • *контекстне навчання;* • *проблемне навчання.*
Процес навчання включає, зокрема, наступне	• *основні методи і засоби протидії віддаленим мережевим атакам на комп'ютерні мережі;* • *Cisco Packet Tracer* • *Побудову комплексної системи захисту для ресурсів комп'ютерних мереж;*
Засоби навчання	• *відео-запис лекції;* • *презентація;* • *підручник;* • *конспект лекцій;* • *різні туторіали.*

Інструменти, обладнання, програмне забезпечення

- *Cisco Packet Tracer, GNS3, Oracle VirtualBox, Visual studio*
- *Microsoft Office;*

Порядок оцінювання програмних результатів навчання/ результатів навчання

Студент може отримати сумарно не більше, ніж 100 балів, за наступні складові:

1) *модульні контролі: 40 балів;*
2) *поточний контроль: 60 балів;*

Розподіл балів:

1) *за модульні контрольні роботи:*
   - *модульний контроль №1 (20 балів):*
     Рівень 1 – 19 запитань по 0.5 балів за кожне.
     Рівень 2 – 6 запитань по 0.9 балів за кожне.
     Рівень 3 – 3 запитання по 1.7 балів за кожне.
   - *модульний контроль №2 (20 балів):*
     Рівень 1 – 19 запитань по 0.5 балів за кожне.
     Рівень 2 – 6 запитань по 0.9 балів за кожне.
     Рівень 3 – 3 запитання по 1.7 балів за кожне.
2) *за лабораторні роботи (48 балів):*

Передбачено по 6 балів за кожну лабораторну роботу; у випадку правильного виконання лабораторної роботи оцінка лінійно залежить від відсотка розуміння коду та виконання завдання. Як альтернатива, студенти можуть виконувати завдання на інших мовах/середовищах логічного/ функціонального програмування за умови попереднього узгодження деталей з викладачем.

в) Передбачено 12 балів за лекційні заняття, за умови відвідування заняття, активної участі студента у обговоренні тем, та ведення конспекту лекцій.

Рекомендована література (основна, допоміжна)

Основна література

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. Технології захисту локальних мереж на основі обладнання CISCO: навч.посіб. /Т.І. Коробейнікова, С.М. Захарченко. – Львів:
Видавництво Львівська політехніка, 2021. – 232 с.

3. Computer Networking: A Top-down Approach, 7th Edition / James F. Kurose, Keith W. Ross – 2020. – 856 с.

4. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.

5. Хорошко В. О.: Проєктування комплексних систем захисту інформації, ISBN: 978-966-941-506-6, Видавництво: Львівська політехніка, 2020р., - 320 с.

6. Євсеєв С.П. , Король О.Г. , Шматко О.В.: Кібербезпека: криптографія з PYTHON, ISBN: 978-617-7519-70-5, Видавництво: Новий світ-2000, 2021р.,- 120 с.
7. Остапов С.Е., Євсеєв С.П., Король О.Г.: Кібербезпека: сучасні технології захисту, ISBN: 978-617-7519-44-6, Видавництво: Новий світ-2000, 2020р.,- 678 с.
8. Taylor & Francis: Cybersecurity: Ambient Technologies, IoT, and Industry 4.0 Implications, ISBN 9780367702168, 2021.,- 222 pages

Допоміжна література

1. Основи інформаційної безпеки [Текст]: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця : ВНТУ, 2018. – 316 с.
2. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. - К., 2013. - 435 с.
3. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник [Текст] / К. : Видавничий дім "КМ Академія", 2003. -244 с.
4. Комп'ютерні мережі. Локальні комп'ютерні мережі. Методичні вказівки до комп'ютерного практикуму. [Текст] / Уклад.: О.Ю. Кулаков, Р.Ю. Берест – К.: НТУУ «КПІ», 2012. – 164 с.
5. Тарнавський Ю. А. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

Інформаційні ресурси в інтернет:

1. CISCO Networking Academy. Режим доступу: https://www.netacad.com/.
2. Закони про кібербезпеку: Режим доступу:
a. https://zakon.rada.gov.ua/laws/show/80/94-D0%B2%D1%80#Text
b. https://zakon.rada.gov.ua/laws/show/2297-17#Text
c. https://zakon.rada.gov.ua/laws/show/3855-12#Text
3. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22. Режим доступу:
4.https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
5. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного

захисту інформації. Передпроектні роботи. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12. 12.2007 р. № 232. Режим доступу: https://tzi.com.ua/downloads/3.1- 001-07.pdf
6. Державна служба спеціального зв'язку та захисту інформації України./www.dsszzi.gov.ua
7. Огляд різноманітних шкідливих програмних засобів/ Viruslist.com

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

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

Вміння комунікувати	• *здатність спілкуватися державною мовою як усно, так і письмово;* • *вміння спілкуватись та писати із використанням англомовної професійної термінології;* • *навички усного спілкування;* • *навички письмового спілкування;* • *вміння писати зрозумілий код.*
Вміння сумісно працювати	• *вміння управляти часом;* • *навички управління проектами;* • *здатність планувати свій час у плані співставлення вимог, власних знань, здібностей і дедлайнів;* • *здатність працювати в команді;* • *навички міжособистісних відношень;* • *вміння надавати рекомендації іншим у коректній формі.*
Здатність до аналізу та синтезу	• *здатність критично мислити;* • *знаходити вихід з складних ситуацій;* • *здатність до навчання;* • *комплексне рішення проблем;* • *критичне мислення.*
Здатність застосовувати знання у практичних ситуаціях	

Поєднання навчання та досліджень

Поєднання навчання і досліджень здобувачів освіти технології має на меті всебічний розвиток студента, засвоєння підходів щодо проведення досліджень спрямованих на вирішення різного типу завдань у процесі професійної діяльності. Основні напрямки наукових досліджень організаційно-правові та нормативні основи захисту інформації в комп'ютерних мережах; основи побудови комплексної системи захисту для ресурсів комп'ютерних мереж; основні тенденції та закономірності розвитку комп'ютерних мереж і засоби їх реалізації; тенденції і закономірності розвитку засобів і методів захисту інформації в комп'ютерних системах та мережах.

Дедлайни та перескладання

Дедлайн здачі лабораторних робіт – до кінця сесії. Здача лабораторних робіт відбувається на парі або під час консультації, дата та час якої гнучко узгоджується між студентом та викладачем.

На здачу кожного з модульних контролів студенту надається одна спроба. Перший модуль здається на будь-якій лекції у квітні, а другий – на передостанній чи останній лекції. Перездача окремого модульного контролю передбачена лише за виключних обставин. При бажанні покращити оцінку за модульну складову оцінювання студент під час сесії звертається до викладача з проханням здати підсумковий контроль (40 балів). При цьому, попередні бали за модульні контролі анулюються.

У разі, якщо здобувач не набрав 60 балів після закінчення сесії, його відправляють на комісію з ліквідації академічної заборгованості. Якщо і тоді здобувач не набирає необхідної кількості балів, то передбачається повторний курс.

Неформальна та інформальна освіта

Студенти мають право на часткове або повне перезарахування предмету за умови написання ними відповідної заяви та надання документів, які підтверджують ті результати навчання, які здобувач отримав (див. положення https://ep3.nuwm.edu.ua/18660/). Зокрема студенти можуть самостійно проходити онлайн-курси на таких навчальних платформах, як Prometheus, Coursera, edEx, edEra, FutureLearn та інших, для наступного перезарахування результатів навчання. Проте доцільно попередньо узгодити з викладачем відповідність обраного онлайн-курсу суті навчальної дисципліни. Деякий перелік підходящих курсів наведено нижче:

- *Coursera – Getting Started with Go (Початок роботи з Go);*
- *Coursera – Functional Programming in Scala (Функціональне програмування в Scala);*
- *Coursera – Kotlin for Java Developers (Kotlin для розробників Java);*
- *Exercism – Prolog;*
- *Swayam – Artificial Intelligence: Knowledge Representation And Reasoning (Штучний інтелект: представлення знань і міркування);*
- *Pluralsight – Code School: On Track with Golang 1 (Школа коду: на шляху до Golang 1);*
- *Pluralsight – F# 6 Fundamentals (Основи F# 6).*

Пошук курсів у зручній формі доступний тут: https://www.classcentral.com/.

Окрім того, *якщо з'являються обставини для здобуття неформальної чи інформальної освіти від викладачів-практиків, то пропонуються ці можливості для студентів; рекомендуються відео-уроки практикуючих програмістів з Youtube тощо.*

Правила академічної доброчесності

Задля запобігання академічної недоброчесності вимагається наступне:

- *кожен студент у групі виконує завдання згідно запропонованого йому варіанту або пропонує свою тему, яку обов'язково узгоджує з викладачем;*
- *студент отримує хоч якусь оцінку лише за умови розуміння коду програми;*
- *студентам забороняється: плагіатити, самоплагіатити, фабрикувати, фальсифікувати, списувати, обманювати та будь-яким чином впливати на викладача, включаючи спроби хабарництва.*

Залежно від виду та ступеня порушення викладач може накладати наступні санкції:

- *усне або письмове зауваження від викладача;*
- *попередження про можливість притягнення до академічної відповідальності;*
- *зниження чи анулювання результатів оцінювання навчального завдання здобувача вищої освіти;*
- *повторне виконання навчального завдання;*
- *виконання іншого навчального завдання;*
- *призначення додаткового навчання з питань академічної доброчесності;*
- *призначення додаткових контрольних заходів (додаткові індивідуальні навчальні завдання, тести тощо);*
- *подання клопотання на ім'я ректора з метою порушення формальної процедури розгляду питання про притягнення студента до відповідальності.*

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

Документи стосовно академічної доброчесності (про плагіат, порядок здачі курсових робіт, кодекс честі студентів, документи Національного агентства стосовно доброчесності) наведені на сторінці «Якість освіти» офіційного сайту НУВГП – http://nuwm.edu.ua/sp/akademichna-dobrochesnistj.

Вимоги до відвідування

Санкції за пропуски пар не передбачені. Студент має право 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. Також викладач розміщує відеозаписи пар на Youtube. 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.

Автор
Старший викладач — Анастасія ШАТНА

Затверджено

Проректор з науково-педагогічної та навчальної роботи — Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №628
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 58E2D9E7F900307B04000000807E2D0054327D00