Інститут телекомунікацій і глобального інформаційного простору НАН України

Відділ інформаційної безпеки

Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Третій (освітньо-науковий)***
Галузь знань	*Галузь F Інформаційні технології*
Спеціальність	*F3 – Комп'ютерні науки*
Освітньо-наукова програма	*Інформаційні технології*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*2 рік, весняний семестр*
Обсяг дисципліни	*90 годин / 3 кредити ЄКТС* *(лекції – 20 год., практичні заняття – 10 год., СРС – 60 год.)*
Семестровий контроль/ контрольні заходи	*залік, модульна контрольна робота*
Розклад занять	*2 год лекційних та 1 год практичних занять на тиждень*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лекції та практичні заняття проводить: *к. т. н. Пустовіт Олександр Сергійович*
Розміщення курсу	https://classroom.google.com/u/0/c/ODY4MTg3NDgyNDE3

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна "Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах" *спрямована на ознайомлення аспірантів з теоретичними основами та практичними аспектами проєктування комплексних систем захисту інформації, методами забезпечення конфіденційності, цілісності та доступності даних, сучасними криптографічними засобами, механізмами контролю доступу, виявлення та протидії кіберзагрозам, а також нормативно-правовими вимогами у сфері інформаційної безпеки. Вивчення дисципліни сприяє формуванню компетентностей щодо аналізу ризиків, розроблення архітектури систем захисту даних та впровадження ефективних рішень для забезпечення безпеки інформаційно-комунікаційних систем і мереж.*

Мета: *набуття аспірантами компетентностей щодо застосування сучасних методів, моделей, технологій і стандартів проєктування систем захисту даних в інформаційно-комунікаційних системах та мережах, проведення аналізу загроз і ризиків інформаційній безпеці, розроблення архітектури комплексних систем захисту інформації та обґрунтування науково-технічних рішень для забезпечення конфіденційності, цілісності, доступності та стійкості інформаційних ресурсів.*

Предмет вивчення – *методи та технології проєктування систем захисту даних в інформаційно-комунікаційних системах і мережах, спрямовані на забезпечення конфіденційності, цілісності, доступності та захищеності інформації від сучасних кіберзагроз.*

Програмні результати навчання: *здатність аналізувати загрози та ризики інформаційної безпеки, проєктувати комплексні системи захисту даних, застосовувати сучасні методи й технології забезпечення конфіденційності, цілісності та доступності інформації, а також проводити наукові дослідження та розробляти інноваційні рішення у сфері захисту даних в інформаційно-комунікаційних системах і мережах.*

Загальні компетентності

ЗК 01 Здатність до абстрактного мислення, аналізу та синтезу
ЗК 03 Здатність до пошуку, оброблення та аналізу інформації з різних джерел
ЗК 04 Здатність розв'язувати комплексні проблеми комп'ютерних наук на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності
ЗК 06 Здатність до набуття концептуальних та методологічних знань в галузі чи на межі галузей знань або професійної діяльності, використання спеціалізованих умінь/навичок і методів, необхідних для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики, безперервного саморозвитку та самовдосконалення

Фахові компетентності

СК 01 Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей.
СК 02 Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.
СК 03 Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень.
СК 06 Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій
СК 08 Здатність дотримуватись академічної та професійної доброчесності, морально-етичних правил поведінки, етики досліджень в академічному середовищі

Програмні результати навчання

ПРН 01 Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.
ПРН 03 Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані
ПРН 04 Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямах

ПРН 05 Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

ПРН 06 Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи

ПРН 10 Відшуковувати, оцінювати та критично аналізувати інформацію щодо поточного стану та трендів розвитку, інструментів та методів досліджень, наукових та інноваційних проєктів з комп'ютерних наук

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна «Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах» вивчається у весняному (четвертому) семестрі. Для її успішного засвоєння необхідні знання, отримані під час вивчення освітніх компонентів, пов'язаних із сучасними інформаційними технологіями, архітектурою та проєктуванням інформаційних систем, комп'ютерними мережами, технологіями обробки даних, програмною інженерією, кібербезпекою та методологією наукових досліджень у галузі комп'ютерних наук. Для вивчення дисципліни «Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах» аспірант має володіти знаннями щодо принципів побудови та функціонування комп'ютерних мереж і розподілених систем, архітектури інформаційно-комунікаційних систем, методів аналізу та проєктування програмного забезпечення, технологій зберігання й обробки даних, основ криптографічного захисту інформації, а також сучасних підходів до забезпечення інформаційної безпеки. Аспірант повинен уміти застосовувати методи системного аналізу, математичного та комп'ютерного моделювання, використовувати сучасні програмні засоби для розроблення, дослідження та оцінювання інформаційних систем і мереж. Результати навчання, отримані під час вивчення дисципліни «Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах», є основою для опанування освітніх компонентів «Стан та перспективи розроблення інформаційних технологій та комп'ютерних систем», «Сучасні методи, моделі та технології оброблення даних в інформаційно-комунікаційних системах та інших дисциплін професійної підготовки, а також для виконання наукових досліджень і написання дисертаційної роботи.

3. Зміст навчальної дисципліни

Тема 1. *Основи проектування та технологія розроблення системи IT систем та мереж, захищених від стороннього кібервпливу*

Тема 2. *Сучасні методи і засоби аналізу та оцінки систем інформаційної безпеки, кіберзахисту інформаційних систем та мереж*

Тема 3. *Технології та інструменти впровадження алгоритмів захисту інформації в системах і мережах*

Тема 4. *Технології адміністрування та експлуатації IT систем і мереж*

Тема 5. *Імплементація постквантових алгоритмів захисту IT систем і мереж*

4. Навчальні матеріали та ресурси

Базова література

1. V. Ustimenko, Graphs in terms of Algebraic Geometry, symbol is computations and secure communications in Post-Quantum world, Wydawnictwo University of Maria-Curie Sklodowska, Lublin, 2022, 212pp. https://www.researchgate.net/publication/359045063
2. V. Ustimenko, O. Pustovit, On families of stream ciphers based on the approximations of regular forests, Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems 2023, Ternopil, Ukraine, Opole, Poland, November 22-24, 2023, 533-547, ISSN 1613-0073, https://ceur-ws.org/Vol-3628/paper30.pdf
3. V. Ustimenko, O. Pustovit, On Symbolic Computations over Arbitrary Commutative Rings via Temporal Jordan-Gauss Graphs and Multivariate Cryptosystems, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, 2025, pp. 405-424, ISSN 1613-0073, https://ceur-ws.org/Vol-3991/paper29.pdf
4. V. Ustimenko, O. Pustovit, On Algebraic Graphs of Large Girth and New Families of Message Authentication Codes (short paper), Proceedings of the Classic, Quantum, and Post-Quantum Cryptography (CQPC), Kyiv, 2025, pp. 76-84, ISSN 1613-0073, https://ceur-ws.org/Vol-4016/short1.pdf
5. Vasyl Ustimenko, Oleksandr Pustovit, Tymofii Svyrydenko, On the stream ciphers based on the hidden algebraic graphs, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, 2025, pp. 358-365, ISSN 1613-0073, https://ceur-ws.org/Vol-4145/short3.pdf

Додаткова література

1. V. Ustimenko, Algebraic graphs and security of digital communications, Institute ofComputer Science, University of Maria Curie Sklodowska in Lublin, 2011, 151 p.
2. V. Ustimenko, U. Romanczuk, Finite geometries, LDPC codes and Cryptography, Lublin, Publication UMCS, 2012.
3. Бурячок В. Л., Хорошко В. О. Технологія прийнятгя рішень у складних соціотехнічних системах : монографія/ В. Л. Бурячок, В. О. Хорошко. - Київ: ДУІКТ, 20 І2. - 344 с.
4. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л.Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В.Лукова-Чуйко І - К.:ДУТ, 2015. - 345 с.
5. Бурячок В.Л. Політика інформаційної безпеки: підручник./ В.Л. Бурячок, Р.В.Грищук, В.О.Хорошка І За заг. ред. докт. техн. наук, проф. В.О.Хорошка. - К.: ПВП «Задруга», 2014. - 222 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

№ п/п	Змістові модулі / теми	Кількість годин, відведених на:			Термін виконання
		лекції	лаб. Заняття	сам. робота.	
1	2	3	4	5	6
Т1	Основи проектування та технологія розроблення системи ІТ систем та мереж, захищених від стороннього кібервпливу *Принципи побудови та вихідні дані для проектування систем захисту ІТ систем. Особливості реалізації атак на захищені ІТ системи та основні уразливості таких систем,*	4	2	12	1-й -3-й тижні

	ризики функціонування захищених ІТ систем в умовах стороннього кібервпливу.				
Т2	Сучасні методи і засоби аналізу та оцінки систем інформаційної безпеки, кіберзахисту інформаційних систем та мереж *Методологія аналізу захищеності інформаційної системи. Стандартизація підходів до забезпечення інформаційної безпеки. Забезпечення інтегральної безпеки інформаційних систем і мереж.*	4	2	12	4-й -6-й тижні
Т3	Технології та інструменти впровадження алгоритмів захисту інформації в системах і мережах *Технологічна модель підсистеми інформаційної безпеки. Технології нижнього рівня захисту інформації в системах інформаційної та кібебезпеки. Концепція захищених віртуальних приватних мереж*	4	2	12	7-й -9-й тижні
Т4	Технології адміністрування та експлуатації ІТ систем і мереж *Удосконалення, модернізація та уніфікація систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації*	4	2	12	10-й -12-й тижні
Т5	Імплементація постквантових алгоритмів захисту ІТ систем і мереж *Впровадження симетричних блокових алгоритмів шифрування, потокові алгоритми шифрування в ІТ системах та мережах. Впровадження протоколів обміну ключів Некомутативної криптографії та постквантової криптографії, що спирається на теорію граток. Впровадження публічних ключів криптографії від багатьох змінних, хаш функції та алгоритми MAC.*	4	2	12	13-й -15-й тижні
МКР	*Модульна контрольна робота*				15-й тиждень
	Всього модуль	**20**	**10**	**60**	

6. Лабораторні заняття

Тема 1. Аналіз кіберзагроз, вразливостей та оцінювання ризиків інформаційно-комунікаційних систем і мереж.

Тема 2. Дослідження методів оцінювання захищеності та аудиту інформаційної безпеки інформаційно-комунікаційних систем і мереж.

Тема 3. Проєктування та моделювання підсистеми захисту інформації в інформаційно-комунікаційних системах і мережах.

Тема 4. Дослідження методів адміністрування, моніторингу та підвищення рівня безпеки інформаційно-комунікаційних систем і мереж.

Тема 5. Експериментальне дослідження та порівняльний аналіз класичних і постквантових криптографічних алгоритмів захисту даних.

7. Самостійна робота аспіранта

№	Вид самостійної роботи	Кількість годин (орієнтовно)
1.	Підготовка до аудиторних занять, опрацювання лекційного матеріалу	20
2.	Підготовка реферату за тематикою індивідуального наукового дослідження	10
3.	Формування наборів даних для аналізу захищеності інформаційно-комунікаційних систем і мереж	5
4.	Проведення розрахунків за сформованими наборами даних	5
5.	Дослідження сучасних методів, моделей, алгоритмів і технологій криптографічного захисту даних, аналіз ефективності їх застосування в інформаційно-комунікаційних системах та мережах за обраною темою дослідження.	10
6.	Формування звіту за результатами дослідження, підготовка презентації виступу	10
	Всього	**60**

Політика та контроль

8. Політика навчальної дисципліни (освітнього компонента)

Вимоги, яких має дотримуватися студент в рамках даної дисципліни:

- правила відвідування занять: відвідування лекцій та практичних занять, а також відсутність на них, не оцінюється. Однак, студентам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання семестрового індивідуального завдання та проводяться контрольні заходи (тести) з поточної оцінки самостійної роботи студентів з засвоєння поточного матеріалу. Останні є складовою частиною поточного рейтингу і проводяться тільки у день проведення відповідних лекцій та практичних занять. Система оцінювання орієнтована на отримання балів за своєчасність виконання студентами практичних та контрольних робіт, а також виконання завдань, які здатні розвинути практичні уміння та навички;
- правила поведінки на заняттях: студент повинен брати участь у розв’язку задач, готувати короткі доповіді;
- захист практичних робіт – захист відбувається у визначені терміні під час аудиторних занять;
- політика щодо академічної доброчесності– політика та принципи академічної доброчесності визначені у Етичному кодексі вченого Інституту телекомунікацій та глобального інформаційного простору НАН України.

9. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Семестровий контроль - залік. Рейтингова система оцінювання результатів навчання передбачає оцінювання заходів поточного контролю з дисципліни впродовж семестру. Рейтингова оцінка здобувача складається з балів, отриманих здобувачем за результатами заходів поточного контролю. Рейтингова оцінка доводиться до здобувачів на передостанньому занятті з дисципліни в семестрі. Здобувачі, які виконали всі умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань

Зі здобувачами, які виконали всі умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить семестровий контроль у вигляді залікової контрольної роботи.

Для посилення зацікавленості здобувачів у якісному виконанні індивідуальних семестрових завдань, передбачених індивідуальним навчальним планом здобувача, рейтингову оцінку, у разі виконання залікової контрольної роботи, можна визначати як суму балів за залікову контрольну роботу та балів за індивідуальне семестрове завдання. У цьому випадку розмір шкали оцінювання залікової контрольної роботи зменшується на максимальне значення балів, передбачених за виконання відповідного індивідуального семестрового завдання.

Після виконання залікової контрольної роботи, якщо оцінка за залікову контрольну роботу більша ніж за рейтингом, здобувач отримує оцінку за результатами залікової контрольної роботи. Якщо оцінка за залікову контрольну роботу менша ніж за рейтингом, то здобувач отримує більшу з оцінок, що отримані за результатами залікової контрольної роботи або за рейтингом.

До відомості семестрового контролю викладач заносить рейтингові бали, отримані здобувачем у семестрі або за результатами виконання залікової контрольної роботи, та оцінку відповідно до цих балів

Критерії нарахування балів:

1. Практичні заняття оцінюються виходячи з максимальної кількості балів - 20 бали кожне:

- «відмінно» – 95 відсотків максимального балу;
- «добре» –75-95 відсотків максимального балу;
- «задовільно» – 60-75 відсотків максимального балу;
- «достатньо» – 50 відсотків – робота виконана, але не захищена.

Умови допуску до підсумкового контролю є зарахування усіх практичних робіт.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

– виконання практичних (лабораторних) робіт;

– виконання самостійної роботи.

За період вивчення дисципліни студент може набрати 100 балів. Їх розподіл між видами робіт наведено в таблиці 1

Таблиця 1

Бали за виконання	Номер практичної роботи або теми					Разом
	1	2	3	4	5	
Практичної роботи	10	10	10	10	10	100
Самостійної роботи	10	10	10	10	10	

2. Залікова контрольна робота оцінюється за такими критеріями:

- «відмінно» – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд;
- «добре» – достатньо повна відповідь (не менше 75% потрібної інформації), що виконана згідно з вимогами до рівня «умінь», або незначні неточності);
- «задовільно» – неповна відповідь (не менше 60% потрібної інформації. що виконана згідно з вимогами до «стереотипного» рівня та деякі помилки);
- «незадовільно» – незадовільна відповідь – 0 балів.

Залікова контрольна робота передбачається у вигляді тесту, критерії оцінювання тесту:

Кількість правильних відповідей	*Відсоток правильних відповідей*	*Оцінка за національною шкалою*	*Оцінка за шкалою ECTS*
48-50	*95-100*	*Відмінно*	*A*
41-47	*82-94*	*Дуже добре*	*B*
37-40	*75-81*	*Добре*	*C*
34-36	*69-74*	*Задовільно*	*D*
30-33	*60-68*	*Достатньо*	*E*
5-29	*10-13*	*Не задовільно*	*FX*

Відповідність рейтингових балів оцінкам за шкалою Інституту та *шкалою ECTS*

Рейтингова оцінка	*Оцінка за національною шкалою*	*Оцінка за шкалою ECTS*
90-100	*Відмінно*	*A*
82-89	*Дуже добре*	*B*
75-81	*Добре*	*C*
69-74	*Задовільно*	*D*
60-68	*Достатньо*	*E*
45-59	*Не задовільно*	*FX*
Невиконання умов допуску до семестрового контролю	*Не допущено*	

10. Додаткова інформація з дисципліни (освітнього компонента)

- *перелік питань, які виносяться на семестровий контроль*
- є можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів Coursera за відповідною тематикою – зараховується додатково до 10 балів до загального рейтингу студента, якщо студент набрав не менше 75 балів за період вивчення курсу та отримав відповідний сертифікат.

Робочу програму навчальної дисципліни (силабус):

Склав: к.т.н. Пустовіт Олександр Сергійович

Затверджено:

Вченою радою Інституту телекомунікацій
і глобального інформаційного простору
НАН України Протокол № 10 від 13 серпня 2026 р.

Введено в дію:
Наказом директора
Наказ від 14 серпня 2026р. № 12