Інститут телекомунікацій і глобального інформаційного простору НАН України

Відділ прикладної інформатики

Інноваційні технології аналізу та синтезу систем захисту інформації

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.ф.-м.н., доцент Худинцев Микола Миколайович*
Розміщення курсу	https://classroom.google.com/_____

Програма навчальної дисципліни

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

Дисципліна "Інноваційні технології аналізу та синтезу систем захисту інформації" *спрямована на ознайомлення аспірантів із сучасними науковими концепціям, поняттями, специфічними інноваційними методами, моделями, їх застосуванням, формування у аспірантів системних наукових компетенцій з аналізу та синтезу інтелектуальних систем захисту інформації і кіберзахисту, здатних функціонувати в умовах динамічних загроз, невизначеності та обмежених ресурсів, аналізу великих даних (Big Data) для вирішення комплексних науково-прикладних завдань забезпечення інформаційної безпеки об'єктів критичної інфраструктури, критичної інформаційної інфраструктури, національної безпеки та оборони. Досліджуються основи побудови систем захисту інформації і кіберзахисту, орієнтованих на застосування інноваційних технологій аналізу і синтезу, поглиблення практичних навичок використання спеціалізованого програмного забезпечення для аналізу та синтезу цих систем.*

Предмет вивчення включає сучасні концепції, математичні моделі та архітектури інтелектуальних систем захисту інформації; методи збору, інтеграції та аналізу різнорідних даних (мережевий трафік, журнали SIEM, телеметрія, OSINT-дані); моделі оцінювання ризиків, вразливостей, сценаріїв атак та ефективності захисних механізмів; методології аналізу та синтезу адаптивних систем захисту на основі сучасних інформаційних технологій; інструментальні засоби для моделювання, верифікації та впровадження інноваційних технічних рішень в системах захисту інформації.

Мета: *набуття здатності продукувати нові ідеї, розв'язувати комплексні науково-прикладні задачі та проблеми в галузі професійної та дослідницько-інноваційної діяльності у сфері*

комп'ютерних наук на основі сформованих фундаментальних знань та практичних навичок із застосування інноваційних моделей, методів та технологій інтелектуального аналізу та синтезу даних, математичного і комп'ютерного моделювання, використовуваних у системах захисту інформації та кіберзахисту, аналізу та синтезу складних систем захисту інформації з урахуванням вимог національної безпеки, оборони, кіберзахисту, екологічної безпеки та природокористування.

Предмет вивчення – *сучасні моделі, методи, алгоритми, технології аналізу та синтезу даних і систем, процеси та способи отримання, представлення, обробки, аналізу, синтезу, передачі, зберігання даних в комп'ютерних системах захисту інформації і кіберзахисту.*

Програмні результати навчання:

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.

СК04 Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проєкти у галузі комп'ютерних наук та дотичних до неї міждисциплінарних проєктах, демонструвати лідерство під час їх реалізації.

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.

ПРН07 Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.

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 «Інноваційні технології аналізу та синтезу систем захисту інформації» вивчається у осінньому (третьому), тому для успішного засвоєння дисципліни необхідні знання з дисциплін «Стан та перспективи розроблення інформаційних технологій та комп'ютерних систем», «Сучасні методи, моделі та технології оброблення даних в інформаційно-комунікаційних системах». Для вивчення дисципліни «Інноваційні технології аналізу та синтезу систем захисту інформації» аспірант має бути знайомий з основами інтелектуального аналізу даних, збору, аналізу та консолідації розподіленої інформації, технологій та методів проектування, інноваційної та дослідницької діяльності, моделями та методами розв'язання інтелектуальних задач, вміти розробляти та використовувати бази даних та знань, мати базові навички з програмування. На результатах навчання з дисципліни «Інноваційні технології аналізу та синтезу систем захисту інформації» базуються такі освітні компоненти, як «Проектування систем захисту даних у інформаційно-комунікаційних системах та мережах», «Інформаційні технології та комп'ютерні системи в задачах екологічної безпеки та природокористування», «Інформаційні системи та технології у задачах національної безпеки та оборони», «Сучасні інформаційні технології та системи підтримки прийняття рішень в управлінні складними системами в умовах невизначеності та ризику» та написання дисертації.

3. Зміст навчальної дисципліни

Тема 1. Концептуальні засади інноваційних технологій аналізу та синтезу систем захисту інформації і кіберзахисту.

Тема 2. Методи та моделі інтелектуального аналізу даних у системах захисту інформації і кіберзахисту.

Тема 3. Моделювання кіберзагроз та оцінювання ризиків у системах захисту інформації і кіберзахисту.

Тема 4. Синтез адаптивних систем захисту інформації та кіберзахисту на основі штучного інтелекту.

Тема 5. Інноваційні інформційні технології захисту критичної інфраструктури та національної безпеки.

4. Навчальні матеріали та ресурси

Базова література

1. Костюк Ю.В., Складанний П.М. Захист інформації в комп'ютерних системах та мережах. Частина І. Теоретичні та методологічні основи захисту інформації в комп'ютерних системах та мережах: підручник. Київ: Київський столичний університет імені Бориса Грінченка, 2026. 401 с. URL: https://elibrary.kubg.edu.ua/id/eprint/56332/1/ZIKSM_part_1_2026_FITM.pdf
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. Системи захисту інформації: підручник. Київ: Київський столичний університет імені Бориса Грінченка, 2025. 887 с. URL: https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf
3. Методи та засоби захисту інформації. ResearchGate, 2024. URL: https://www.researchgate.net/publication/378457210_METODI_TA_ZASOBI_ZAHISTU_INFORMACII
4. Державний університет інформаційно-комунікаційних технологій. Системи захисту інформації: навчально-методичні матеріали. Київ: ДУІКТ. URL: https://duikt.edu.ua/ua/lib/1/category/2404/view/2230.

Додаткова література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
3. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
4. Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021
5. Стратегія інформаційної безпеки України: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021
6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п
7. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження КМУ від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р
8. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2023.
9. Про затвердження Вимог до захисту інформації в інформаційних системах: Наказ Держспецзв'язку від 26.05.2022 № 272. URL: https://zakon.rada.gov.ua/rada/show/v0272857-22
10. Khudyntsev M.M., Palazhchenko I.L. Cybersecurity maturity models for cybersecurity assessment in critical infrastructure. Environmental Safety and Natural Resources. 2024. Т. 52, № 4. С. 122–134. DOI: https://doi.org/10.32347/2411-4049.2024.4.122-134

11. Khudyntsev M., Khomenko O., Klymenkov O. Methodological basis of cyberinsurance risk assessment. Environmental Safety and Natural Resources. 2026. Т. 58, № 2. С. 251–261. DOI: https://doi.org/10.32347/2411-4049.2026.2.251-261
12. Khudyntsev M., Lebid O., Bychenok M., Zhylin A., Davydiuk A. Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. In: Dovgyi S., Trofymchuk O., Ustimenko V., Globa L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham, 2023. DOI: https://doi.org/10.1007/9783031468803_17
13. Khudyntsev M., Davydiuk A., Lebid O., Trofymchuk O., Zhylin A. Cybersecurity Indices: Review and Classification. CPITS II. 2021. С. 117–126. URL: https://api.semanticscholar.org/CorpusID:251724776

Інформаційні ресурси

1. Національний репозитарій академічних текстів НАН України. URL: https://harvester.nas.gov.ua
2. Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua
3. MITRE ATT&CK Framework. URL: https://attack.mitre.org
4. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov
5. ENISA (European Union Agency for Cybersecurity). URL: https://www.enisa.europa.eu
6. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). URL: https://ccdcoe.org
7. CISA – Critical Infrastructure Security. URL: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
8. IEEE Xplore Digital Library – Cybersecurity & Data Analytics. URL: https://ieeexplore.ieee.org
9. arXiv.org – Cryptography and Security. URL: https://arxiv.org/list/cs.CR
10. GitHub – Open Source Cyber Security Tools. URL: https://github.com/topics/cybersecurity
11. OWASP – Open Web Application Security Project. URL: https://owasp.org

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Таблиця 1

№ п/п	Змістові модулі / теми	Кількість годин, відведених на:			Термін виконання
		лекції	лаб. заняття	сам. робота.	
1	2	3	4	5	6
Т1	**Концептуальні засади інноваційних технологій аналізу та синтезу систем захисту інформації і кіберзахисту (Тема 1)** *Розглядаються базові поняття, класифікація та еволюція систем захисту інформації в умовах динамічних кіберзагроз. Висвітлюються сучасні наукові концепції, методологічні підходи до аналізу стану інформаційної безпеки, принципи побудови інтелектуальних систем підтримки прийняття рішень (СППР) для завдань національної безпеки та оборони. Окрему увагу приділено аналізу вітчизняного та міжнародного досвіду формування систем кіберзахисту критичної інфраструктури.*	4	2	12	1-й -3-й тижні

Т2	**Методи та моделі інтелектуального аналізу даних у системах захисту інформації і кіберзахисту (Тема 2)** *Тема присвячена сучасним методам збору, очищення, інтеграції та аналізу великих масивів різнорідних даних (Big Data) для потреб кібербезпеки. Розглядаються моделі машинного та глибинного навчання для виявлення аномалій, індикаторів компрометації (IoC) та поведінкових патернів у мережевому трафіку, журналах SIEM-систем, телеметрії та даних відкритих джерел (OSINT). Аналізуються методи статистичної обробки даних про кіберінциденти та підходи до формування індексів кібербезпеки для прогнозного моделювання.*	4	2	12	4-й -6-й тижні
Т3	**Моделювання кіберзагроз та оцінювання ризиків у системах захисту інформації і кіберзахисту (Тема 3)** *Досліджуються математичні та імітаційні моделі кіберзагроз, вразливостей та сценаріїв атак на основі тактик і технік MITRE ATT&CK. Розглядаються методи оцінювання ризиків інформаційної безпеки, побудови профілів супротивника, аналізу поверхні атак. Висвітлюються підходи до моделювання динаміки кіберінцидентів, зокрема з використанням мережевих та економічних індексів кібербезпеки, що дозволяє формувати багатокритеріальні системи оцінки ефективності захисних механізмів.*	4	2	12	7-й -9-й тижні
Т4	**Синтез адаптивних систем захисту інформації та кіберзахисту на основі штучного інтелекту (Тема 4)** *Досліджується методологія синтезу активних, адаптивних та самонавчальних систем захисту інформації, здатних функціонувати в умовах динамічного загрозливого середовища. Розглядаються архітектурні принципи побудови інтелектуальних систем виявлення вторгнень (IDS/IPS), прогнозуючих моделей кібератак, автоматизованих систем реагування на інциденти. Аналізуються підходи до синтезу захисних політик на основі теорії ігор, еволюційних алгоритмів, федеративного навчання та агентного моделювання. Висвітлюються питання оцінювання ефективності синтезованих захисних механізмів за комплексом показників.*	4	2	12	10-й -12-й тижні
Т5	**Інноваційні інформаційні технології захисту критичної інфраструктури та національної безпеки (Тема 5)** *Комплексно досліджуються проблеми захисту об'єктів критичної інфраструктури з використанням інноваційних технологій аналізу даних, геоінформаційних систем (ГІС) та інтелектуальних СППР. Розглядаються моделі оцінювання рівня*	4	2	12	13-й -15-й тижні

	кібербезпеки національної системи кібербезпеки, галузеві підходи до захисту енергетичного, транспортного, телекомунікаційного та інших секторів критичної інфраструктури. Висвітлюються питання формування індексів кібербезпеки, моделей зрілості кібербезпеки (cybersecurity maturity models) та розробки методологічних засад їх застосування для накопичення статистичних даних про кіберінциденти з метою прогнозного моделювання та підвищення кіберстійкості держави.				
МКР	*Модульна контрольна робота*				15й тиждень
	Всього модуль	**20**	**10**	**60**	

6. Практичні/Лабораторні заняття

Тема 1. Концептуальні засади інноваційних технологій аналізу та синтезу систем захисту інформації і кіберзахисту

Мета заняття: закріпити теоретичні знання щодо еволюції систем захисту інформації, базових принципів інформаційної безпеки, а також навчитися аналізувати міжнародні стандарти та національне законодавство у сфері кібербезпеки.

Приклади завдань:

1. Провести порівняльний аналіз міжнародних стандартів (ISO/IEC 27001, NIST CSF, COBIT, GDPR) та визначити їх застосовність для побудови систем кіберзахисту критичної інфраструктури України.
2. Здійснити огляд чинного законодавства України у сфері кібербезпеки (Закони «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах») та розробити структурно-логічну схему нормативного регулювання.
3. Проаналізувати основні кіберінциденти останніх років (на прикладі атак на критичну інфраструктуру) та сформулювати висновки щодо еволюції загроз і методів протидії.

Інструменти: відкриті бази даних кіберінцидентів (CVE Details, CERT-UA), тексти законодавчих актів (rada.gov.ua), програмне забезпечення для побудови схем та діаграм.

Очікувані результати: здатність класифікувати загрози, обґрунтовувати вибір стандартів, розуміння сучасної парадигми кібербезпеки та нормативних вимог до систем захисту інформації.

Тема 2. Методи та моделі інтелектуального аналізу даних у системах захисту інформації і кіберзахисту

Мета заняття: набути практичних навичок застосування методів інтелектуального аналізу даних (Big Data, машинне навчання, статистичний аналіз) для виявлення аномалій та індикаторів компрометації в кіберпросторі.

Приклади завдань:

1. На основі наданого набору даних (журнали SIEM, мережевий трафік) провести попередню обробку (очищення, нормалізацію, агрегацію) даних з використанням Python (бібліотеки Pandas, NumPy) або спеціалізованих платформ (ELK Stack, Splunk).
2. Розробити та реалізувати модель машинного навчання (наприклад, класифікатор на основі Random Forest або Isolation Forest) для виявлення аномалій у мережевому трафіку. Провести оцінку якості моделі (матриця помилок, точність, повнота, F1-міра).

3. Здійснити статистичний аналіз даних про кіберінциденти та побудувати часові ряди для прогнозування інтенсивності атак. Оцінити застосовність індексів кібербезпеки для прогнозного моделювання.

Інструменти: мова Python (Scikit-learn, Pandas, Matplotlib, Seaborn), SIEM-системи (Elastic Stack, Splunk), статистичні пакети (R, SPSS).

Очікувані результати: володіння методами обробки та аналізу великих даних, здатність розробляти та оцінювати моделі виявлення аномалій, вміння інтерпретувати результати статистичного аналізу для прийняття рішень у сфері кібербезпеки.

Тема 3. Моделювання кіберзагроз та оцінювання ризиків у системах захисту інформації і кіберзахисту

Мета заняття: опанувати практичні методи побудови моделей кіберзагроз, оцінювання ризиків та формування багатокритеріальних систем оцінки ефективності захисних механізмів.

Приклади завдань:

1. На основі обраного сценарію атаки (згідно з MITRE ATT&CK) побудувати ланцюг кібератаки (Cyber Kill Chain) та визначити ключові вразливості на кожному етапі.
2. Виконати оцінку ризиків для заданої інформаційної системи з використанням кількісних методів (наприклад, FAIR) або якісних підходів (матриця ймовірності та впливу). Розробити рекомендації щодо мінімізації виявлених ризиків.
3. Розробити та обґрунтувати систему показників для оцінювання ефективності захисних механізмів (зокрема з використанням мережевих та економічних індексів кібербезпеки).

Інструменти: MITRE ATT&CK Navigator, спеціалізовані програмні засоби для оцінки ризиків (RiskWatch, Isograph), MS Excel (для розрахунків показників).

Очікувані результати: здатність моделювати сценарії кібератак, виконувати оцінку ризиків, обґрунтовувати вибір контрзаходів та формувати системи показників для моніторингу ефективності захисту.

Тема 4. Синтез адаптивних систем захисту інформації та кіберзахисту на основі штучного інтелекту

Мета заняття: навчитися застосовувати методологію синтезу адаптивних систем захисту з використанням методів штучного інтелекту, теорії ігор та агентного моделювання.

Приклади завдань:

1. Розробити архітектуру інтелектуальної системи виявлення вторгнень (IDS) з використанням методів глибинного навчання (наприклад, нейронні мережі для аналізу мережевих пакетів). Провести експериментальне дослідження на основі відкритих наборів даних (NSL-KDD, CIC-IDS).
2. Змоделювати поведінковий патерн супротивника та синтезувати адаптивну захисну політику на основі теорії ігор (побудова матриці гри та визначення оптимальних стратегій захисту).
3. Розробити концепцію агентної моделі системи захисту, де агенти реагують на зміни загрозливого середовища та координаційно взаємодіють для прийняття рішень (симуляція у середовищі NetLogo або AnyLogic).

Інструменти: Python (TensorFlow, PyTorch, Scikit-learn), платформи для моделювання (NetLogo, AnyLogic), набори даних для IDS (NSL-KDD, CIC-IDS).

Очікувані результати: розуміння принципів побудови інтелектуальних систем виявлення вторгнень, здатність синтезувати адаптивні політики захисту на основі ігрових та агентних підходів, вміння оцінювати ефективність синтезованих рішень.

Тема 5. Інноваційні інформційні технології захисту критичної інфраструктури та національної безпеки

Мета заняття: набути практичних навичок застосування інноваційних технологій аналізу даних, геоінформаційних систем та інтелектуальних СППР для захисту об'єктів критичної інфраструктури.

Приклади завдань:

1. Розробити концептуальну модель системи кіберзахисту для визначеного об'єкта критичної інфраструктури (на вибір: енергетичний, транспортний, телекомунікаційний сектор) з використанням підходу «захист у глибину» (Defense-in-Depth).
2. З використанням геоінформаційних систем (ArcGIS, QGIS) провести просторовий аналіз розташування об'єктів критичної інфраструктури та розробити карту кіберзагроз для регіону. Інтегрувати ГІС-дані з системою підтримки прийняття рішень (СППР).
3. Розробити модель оцінювання зрілості кібербезпеки (cybersecurity maturity model) для об'єкта критичної інфраструктури (на основі NIST CSF або іншої методології). Провести оцінку поточного рівня зрілості та сформувати рекомендації щодо його підвищення.
4. Створити прототип інформаційно-аналітичної панелі (dashboard) для моніторингу стану кібербезпеки критичної інфраструктури на основі інтеграції даних з SIEM, ГІС та відкритих джерел.

Інструменти: ГІС-системи (ArcGIS, QGIS), платформи для візуалізації даних (Tableau, Power BI), інструменти для побудови СППР (Microsoft Power Platform, IBM CPLEX), методики оцінки зрілості (NIST CSF, CMMI).

Очікувані результати: здатність проєктувати системи захисту для об'єктів критичної інфраструктури, виконувати просторовий аналіз загроз, оцінювати рівень кібербезпеки на основі моделей зрілості та формувати рекомендації для підвищення кіберстійкості держави.

7. Самостійна робота аспіранта

Таблиця 2

№	Вид самостійної роботи	Кількість годин
1.	Підготовка до аудиторних занять	20
2.	Написання реферату за темою індивідуального дослідження	10
3.	Формування наборів даних для аналізу	5
4.	Проведення розрахунків за обраною темою	5
5.	Дослідження за обраною темою	5
6	Доповідь по темі	10
7	Формування звіту за результатами дослідження, підготовка презентації виступу	5
	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 (лабораторних) 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, наведено у Додатку.*
- є можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів Coursera, Alison 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.ф.-м.н., доцент Худинцев Микола Миколайович***

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 2026 р. № 12

Додаток

Перелік питань (тем), які виносяться на семестровий контроль

1. Еволюція інформаційної безпеки: основні етапи розвитку, ключові історичні інциденти та їх вплив на формування сучасної парадигми кібербезпеки.
2. Базові принципи захисту інформації (CIAAN-модель): сутність конфіденційності, цілісності, доступності, автентичності та невідмовності. Практичні механізми їх реалізації.
3. Міжнародні стандарти та рамкові моделі безпеки: порівняльний аналіз ISO/IEC 27001, NIST CSF, COBIT, DORA, GDPR. Сфери застосування та вимоги.
4. Національне законодавство України у сфері кібербезпеки: огляд ключових законів (Про основні засади забезпечення кібербезпеки, Про критичну інфраструктуру, Про захист інформації в ІКС). Структура та функції національної системи кібербезпеки.
5. Політика інформаційної безпеки підприємства: структура, етапи розробки, впровадження та моніторинг. Взаємозв'язок з організаційною структурою та бізнес-процесами.
6. Класифікація кіберзагроз та шкідливого програмного забезпечення: види загроз, моделі супротивників, типи шкідливого ПЗ (віруси, трояни, руткіти, ботнети, ransomware) та методи їх поширення.
7. Інноваційні концепції захисту інформації: принципи Zero Trust, «захист у глибину» (Defense-in-Depth), безпека як код (Security as Code). Порівняльний аналіз та умови застосування.
8. Методи збору, очищення та попередньої обробки великих даних (Big Data) для потреб кібербезпеки: джерела даних, проблеми якості даних, етапи попередньої обробки.
9. Архітектура систем обробки та зберігання великих даних: Data Lake, Data Mesh, потокова обробка, розподілені файлові системи (HDFS). Застосування для кібермоніторингу.
10. Моделі машинного навчання для виявлення аномалій: методи навчання з учителем, без учителя та напівавтоматичні підходи. Класифікація моделей (дерева рішень, SVM, нейронні мережі, isolation forest).
11. Методи глибинного навчання (Deep Learning) у кібербезпеці: згорткові та рекурентні нейронні мережі для аналізу мережевого трафіку, виявлення аномалій та прогнозування атак.
12. Поведінковий аналіз та виявлення індикаторів компрометації (IoC): типи IoC (мережеві, файлові, поведінкові), методи їх виявлення та автоматизація процесу.
13. Статистичні методи обробки даних про кіберінциденти: аналіз часових рядів, методи прогнозування інтенсивності атак, оцінювання трендів та сезонності.
14. Інноваційні методи аналізу неструктурованих даних з відкритих джерел (OSINT): методи збору, обробки та аналізу текстових даних, соціальних мереж, веб-ресурсів для виявлення кіберзагроз.
15. Семантичний та контекстний аналіз даних для виявлення прихованих загроз: методи обробки природної мови (NLP), моделі трансформерів (BERT, GPT) для аналізу загроз у відкритих джерелах.
16. Графові моделі та аналіз зв'язків у кібербезпеці: застосування теорії графів для моделювання взаємодії між об'єктами, виявлення прихованих зв'язків та прогнозування атак.
17. Адаптивне навчання моделей у динамічному середовищі кіберзагроз: методи online learning, transfer learning, федеративного навчання для швидкої адаптації до нових типів атак.
18. Індекси кібербезпеки: огляд існуючих індексів (Global Cybersecurity Index, Cybersecurity Exposure Index), методи їх формування та застосування для порівняльного аналізу та прогнозного моделювання.
19. Математичні моделі кіберзагроз: формальні моделі (Белла-Лападули, Біба), моделі потоку інформації, моделі атак на основі графів та мереж Петрі.
20. Імітаційне моделювання сценаріїв кібератак: методи Монте-Карло, агентне моделювання, дискретно-подієве моделювання. Програмні засоби для імітаційного моделювання.
21. Тактики, техніки та процедури (TTPs) сучасних кібератак: структура та використання бази знань MITRE ATT&CK. Побудова профілів супротивника та аналіз поверхні атак.
22. Методології оцінювання ризиків інформаційної безпеки: кількісні (FAIR) та якісні (матриця ймовірності та впливу) підходи. Визначення та класифікація активів, загроз, вразливостей.
23. Багатокритеріальні системи оцінки ефективності захисних механізмів: показники ефективності (KPI) для систем захисту, методи згортання критеріїв, прийняття рішень в умовах багатокритеріальності.
24. Моделі зрілості кібербезпеки (Cybersecurity Maturity Models): огляд моделей (NIST CSF Maturity, C2M2, CMMC), методики оцінювання та шляхи підвищення рівня зрілості.

25. Архітектурні принципи побудови інтелектуальних систем виявлення вторгнень (IDS/IPS): типи IDS/IPS (мережеві, хост-базовані), методи виявлення (сигнатурні, поведінкові, гібридні), сучасні тенденції розвитку.
26. Прогнозуючі моделі кібератак: методи прогнозування на основі аналізу часових рядів, машинного навчання та гібридних підходів. Оцінювання якості прогнозів.
27. Інноваційні методи синтезу систем виявлення вторгнень: глибинні нейронні мережі (CNN, LSTM, Autoencoders), ансамблеві методи (Random Forest, Gradient Boosting), гібридні моделі для підвищення точності виявлення.
28. Автоматизовані системи реагування на інциденти (SOAR): архітектура, функціональні компоненти, плейбуки автоматизації, інтеграція з SIEM та IDS/IPS.
29. Синтез захисних політик на основі теорії ігор: моделювання взаємодії захисника та супротивника, визначення оптимальних стратегій, застосування для динамічного управління доступом.
30. Застосування еволюційних алгоритмів та федеративного навчання для синтезу захисних механізмів: принципи, переваги, обмеження та приклади застосування.
31. Інноваційні методи аналізу даних для виявлення APT-атак: методи аналізу ланцюгів атак, виявлення аномалій у поведінці користувачів (UBA/UEBA), машинне навчання для детекції складних загроз.
32. Синтез систем виявлення аномалій на основі глибинного навчання: архітектури автоенкодерів, GAN (Generative Adversarial Networks) для виявлення відхилень у поведінці мережі та користувачів.
33. Гібридні моделі для аналізу та синтезу систем захисту: комбінування методів аналізу даних, машинного навчання, агентного моделювання та експертних систем для комплексного захисту інформації.
34. Поняття та класифікація об'єктів критичної інфраструктури: визначення, сектори критичної інфраструктури (енергетика, транспорт, зв'язок, фінанси), критерії віднесення.
35. Галузеві підходи до захисту критичної інфраструктури: особливості захисту енергетичного, транспортного, телекомунікаційного та інших секторів. Специфічні загрози та методи протидії.
36. Застосування геоінформаційних систем (ГІС) для аналізу загроз критичній інфраструктурі: просторовий аналіз, картографування загроз, інтеграція з СППР.
37. Інноваційні технології захисту критичної інфраструктури: застосування технологій IoT/IIoT безпеки, захисту SCADA/ICS-систем, впровадження хмарних та туманних обчислень для моніторингу стану об'єктів.
38. Методологічні засади формування індексів кібербезпеки для національної системи: структура індексу, методи розрахунку, застосування для моніторингу та порівняльного аналізу.
39. Інтелектуальні системи підтримки прийняття рішень (СППР) у сфері національної безпеки та оборони: архітектура, функції, джерела даних, приклади застосування для управління кіберзахистом.
40. Стратегії підвищення кіберстійкості держави: комплексний підхід (технічний, організаційний, правовий, освітній), міжнародна співпраця, роль державно-приватного партнерства.
41. Інноваційні методи аналізу та візуалізації великих даних для систем підтримки прийняття рішень: інтерактивна візуалізація, дашборди для моніторингу кіберзагроз, аналітика реального часу.
42. Синтез оптимальних структур систем захисту інформації: методи оптимізації, багатокритеріальний вибір архітектурних рішень, оцінка вартості та ефективності захисних механізмів.
43. Застосування технологій штучного інтелекту для аналізу вразливостей та синтезу контрзаходів: автоматизоване сканування вразливостей, генерація рекомендацій, предиктивна аналітика.
44. Інноваційні підходи до управління інцидентами кібербезпеки: автоматизація процесів, використання AI для класифікації та пріоритезації інцидентів, адаптивне навчання систем реагування.
45. Перспективи розвитку технологій аналізу та синтезу систем захисту інформації: вплив квантових обчислень, розвиток технологій штучного інтелекту, нові виклики та напрями досліджень.

Рівень складності: питання 1–7, 24–26, 34–36 – базові; питання 8–13, 18–23, 37–40 – середні; питання 14–17, 27–33, 41–45 – поглиблені (інноваційні методи, аналіз та синтез); питання відповідають вимогам PhD-рівня.
Акцент на інноваційність: питання 14–17, 27, 31–33, 37, 41–45 спрямовані на розвиток здатності до аналізу, синтезу та застосування інноваційних підходів у сфері кібербезпеки