***МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ***
***Харківський національний університет внутрішніх справ***
***Факультет № 6***
***Кафедра кібербезпеки та DATA–технологій***

**ЗАТВЕРДЖЕНО**
На засіданні кафедри
кібербезпеки та DATA-технологій
протокол № 12 від 15 грудня 2023 р.
Завідувач кафедри
_____ **Юрій ГНУСОВ**

**Лучик Василь Єфремович**

# МОДЕЛЮВАННЯ СКЛАДНИХ НЕЛІНІЙНИХ ПРОЦЕСІВ В КІБЕРБЕЗПЕЦІ(ОК.03)

## ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| | |
|---|---|
| **Кафедра** | кібербезпеки та DATA–технологій (http://univd.edu.ua/uk/dir/1740/kafedra-informatsiynykh-tekhnologiy-ta-kiberbezpeky) |
| **Контактний телефон** | +38 057 7398085 (роб.) |
| **E-mail** | moj@univd.edu.ua |
| **Офіційна назва освітньої програми** | Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems) |
| **Рівень вищої освіти** | Другий (магістерський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій |

| | |
|---|---|
| | Європейського простору вищої освіти) |
| **Галузь знань** | 12 Інформаційні технології |
| **Спеціальність** | 125 Кібербезпека та захист інформації |
| **Спеціалізація** | Безпека інформаційних та комунікаційних систем |
| **Статус дисципліни** | Нормативна компонента освітньо-наукової програми, вивчається в 2 семестрі І курсу навчання |
| **Мова викладання** | Українська |
| **Обсяг дисципліни в кредитах ECTS/годинах** | 3 кредити ECTS (загальний обсяг – 90 год.) |
| | - аудиторна робота (денна/заочна): 40/16 год.,<br>з них: |
| | лекції: 16/6 год. |
| | лабораторні заняття: 0 год. |
| | практичні заняття: 24/4 год. |
| | семінарські заняття: 0 год. |
| | самостійна робота: 50/80 год. |
| **Час і місце проведення навчальної дисципліни** | Аудиторія та час проведення заняття згідно розкладу |
| **Консультації з навчальної дисципліни** | Аудиторні консультації: аудиторія згідно графіку консультацій.<br>Он-лайн-консультації: письмово в системі дистанційного навчання Moodle або електронною поштою викладача |
| **Мета вивчення дисципліни** | викладання дисципліни " Моделювання складних нелінійних процесів в кібербезпеці": формування у студентів компетентностей щодо принципів побудови та оцінки моделей складних нелінійних процесів різного походження, що використовуються на різних етапах аналізу, розробки та застосування систем технічного захисту інформації, захисту в інформаційно-комунікаційних мережах та кібербезпеці |
| **Завдання вивчення дисципліни** | Дослідження чинних стандартів у сфері забезпечення безпеки інформації. |
| **Форми та види проведення навчальних занять** | Форма навчання – денна або заочна.<br>Види навчальних занять: лекції, практичні, самостійна робота. |
| **Самостійна робота** | Опрацювання рекомендованої літератури, підготовка тез доповідей до конференційта наукових статей |
| **Необхідне** | Мультимедійне обладнання (ноутбук та проектор), |

| | |
|---|---|
| **обладнання** | комп'ютерне забезпечення з виходом у мережу Інтернет. |
| **Індивідуальні завдання** | Наукові доповіді, реферати |
| **Контроль** | Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: залік. |
| **Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності** | Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки<br>ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.<br>ЗК3. Здатність проводити дослідницьку та/або інноваційну діяльність<br>ФК 1. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених інформаційно-телекомунікаційних систем (ІТС), каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації. |

**ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ**

**ЛЕКЦІЙНІ ЗАНЯТТЯ**

**Тема 1. Методи моделювання складних нелінійних процесів в кібербезпеці**

1. Методи і моделі систем. Інформаційний підхід в теорії систем.
2. Застосування загальної теорії систем. Складні системи.
3. Математичні моделі систем керування.
4. Методи та моделі теорії оптимальних процесів.
5. Моделювання нелінійних процесів та детермінований хаос.
6. Фрактальні моделі нелінійних процесів.

**Тема 2. Оптимізація моделей складних нелінійних процесів та їх застосування в кібербезпеці**

1. Реконструкція моделей нелінійних динамічних систем.
2. Фрактальний аналіз часових рядів.
3. Адаптивне прогнозування сигналів та стану об'єктів.
4. Структурно-параметрична ідентифікація та прогнозування нелінійних динамічних процесів.
5. Моделі моніторингу амо подібного трафіку в ІКМ для систем виявлення атак
6. Оцінювання, ідентифікація та прогнозування амо подібного трафіку в ІКМ для систем виявлення атак

| | |
|---|---|
| 7. Кіберфізична система моделювання захисту акустичної інформації від витоку<br>8. Інтелектуальне прогнозування мовного сигналу в системі конфіденційного зв'язку | |
| **ПРАКТИЧНІ ЗАНЯТТЯ** | |
| **Тема 1. Методи моделювання складних нелінійних процесів в кібербезпеці**<br>1. Імітаційне моделювання супутникової системи зв'язку<br>2. Вейвлет перетворення векторних сигналів<br>3. Банки вейвлет фільтрів | |
| **Тема 2. Оптимізація моделей складних нелінійних процесів та їх застосування в кібербезпеці**<br>1. Оптимізація моделі адаптивною системою нечіткого висновку<br>2. Адаптивна нечітка оптимізація моделі динамічного нелінійного процесу<br>3. Нейромережева система оптимізації процеса з прогнозом | |
| **Результати навчання** | РН 2. Знання та розуміння законодавчої та нормативно-правової бази, вимог відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності<br>РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.<br>РН 12. Здатність здійснювати поліцейську діяльність із протидії кіберзлочинності<br>РН 13. Здатність проводити кримінальну розвідку при вирішенні задач поліцейської діяльності<br>РН 16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.<br>РН 17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати |

| | |
|---|---|
| | навчання.<br>РН 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.<br>РН 23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. |
| **Критерії оцінювання** | Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:<br>- поточний контроль - 50 балів;<br>- підсумковий контроль - 50 балів.<br>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.<br>Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені). |

**ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS**

| **Оцінка в балах** | **Оцінка за національною шкалою** | **Оцінка за шкалою ECTS** | |
|---|---|---|---|
| | | **Оцінка** | **Пояснення** |
| **97-100** | Відмінно (“зараховано”) | A | **„Відмінно”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом |

| | | | |
|---|---|---|---|
| **94-96**<br>**90-93** | | | сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою. |
| **85-89**<br>**80-84** | Добре (“зараховано”) | B | **„Дуже добре”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками. |
| **75-79** | | C | **„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками. |
| **70-74**<br>**65-69** | Задовільно (“зараховано”) | D | **„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками. |
| **60-64** | | E | **„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки. |

| | | | |
|---|---|---|---|
| **40-59** | Незадовільно („не зараховано”) | FX | **„Умовно незадовільно”** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки |
| **21-40** | | F | **„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками. |
| **1-20** | | F | **„Безумовно незадовільно”** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки |
| **Орієнтовний перелік питань до заліку (екзамену)** | | 1. Методи і моделі систем.<br>2. Інформаційний підхід в теорії систем.<br>3. Застосування загальної теорії систем.<br>4. Складні системи.<br>5. Математичні моделі систем керування.<br>6. Методи та моделі теорії оптимальних процесів.<br>7. Моделювання нелінійних процесів.<br>8. Детермінований хаос.<br>9. Фрактальні моделі нелінійних процесів.<br>10. Реконструкція моделей нелінійних динамічних систем.<br>11. Фрактальний аналіз часових рядів.<br>12. Адаптивне прогнозування сигналів та стану | |

| | |
|---|---|
| | об’єктів.<br>13. Структурно-параметрична ідентифікація нелінійних динамічних процесів.<br>14. Прогнозування нелінійних динамічних процесів.<br>15. Моделі моніторингу самоподібного трафіку в ІКМ для систем виявлення атак<br>16. Оцінювання, ідентифікація та прогнозування самоподібного трафіку в ІКМ для систем виявлення атак<br>17. Кіберфізична система моделювання захисту акустичної інформації від витоку<br>18. Інтелектуальне прогнозування мовного сигналу в системі конфіденційного зв’язку<br>19. Імітаційне моделювання супутникової системи зв’язку<br>20. Вейвлет перетворення векторних сигналів<br>21. Банки вейвлет фільтрів<br>22. Оптимізація моделі адаптивною системою нечіткого висновку<br>23. Адаптивна нечітка оптимізація моделі динамічного нелінійного процесу<br>24. Нейромережева система оптимізації процесу з прогнозом |
| **Рекомендована література** | |
| **Основна** | 1. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в керуванні, кібербезпеці, телекомунікаціях: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна. – Міністерство освіти і науки України, Національний технічний університет «Дніпровська політехніка». – Дніпро, НТУ «ДП», 2020. – 531 с.<br>2. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. — К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. — 297 с.<br>3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.<br>4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – |

| | |
|---|---|
| | К.: ДУТ, 2015. – 288 с.<br>5. Корнієнко В.І.. Теорія систем керування: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна, В.П. Щокін. – М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2017. – 497 с. – ISBN 978-966-350-650-0. 2.<br>6. Gusev O.Yu. Theory of adaptive filtration: tutorial / O.Yu.Gusev, V.M.Gorev, V.I.Kornienko; Ministry of Education and Science of Ukrain, National Technical University “Dnipro polytechnic”.- Dnipro: NTU “DP”, 2019.- 156 p. |
| **Допоміжна література** | 7. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г Даник, П.П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. –228 с.<br>8. Diks C. Nonlinear Time Series Analysis: Methods and Applications / C. Diks. – World Scientific Press, 1999. – 180 pp.<br>9. Глибовець М. М. Штучний інтелект : підручник для студ. вищих навч.закладів / М. М. Глибовець, О.В. Олецький. – К. : КМ Академія, 2002. – 369 с.<br>10. Зайченко, Ю.П. Нечіткі моделі і методи в інтелектуальних системах. - К: Слово, 2008. – 344 с. |
| **Інформаційні ресурси в Інтернеті** | 11. Каталог національних стандартів та кодексів усталеної практики. URL: https://katalog.uas.org.ua.<br>12. Operating Systems and You: Becoming a Power User. URL: https://www.coursera.org/learn/os-power-user/home/welcome<br>13. System Administration and IT Infrastructure Services. URL: https://www.coursera.org/learn/system-administration-it-infrastructure-services?specialization=google-it-support.<br>14. Cisco Networking Academy. Cisco Packet Tracer URL: https://www.netacad.com/courses/packet-tracer.<br>15. Мережна академія Cisco. URL: https://www.cisco.com/c/uk_ua/index.html.<br>16. Освітні дистанційні курси Cisco. URL: https://edu-cisco.org. |