НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол №9 від «26» 06. 2026 р.)

# Ф-КАТАЛОГ
# ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
# ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

**для здобувачів ступеня магістра за освітньою програмою**
**«Системи технічного захисту інформації»,**
**за спеціальністю F5 Кібербезпека та захист інформації**

УХВАЛЕНО:

Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол №8 від «15» 06 2026 р.)

Київ – 2026

Дисципліни вільного вибору студентів (вибіркові дисципліни), спрямовані на забезпечення загальних та фахових компетенцій за спеціальністю. Обсяг вибіркових навчальних дисциплін становить не менше 25% від загальної кількості кредитів ЄКТС. Вибір дисциплін регламентується «Положенням про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/node/185).

Ф-Каталог містить анотований перелік вибіркових дисциплін, які, відповідно до освітньої програми, беруть участь у формуванні фахових компетентностей. Вибір дисциплін здійснюється у весняному семестрі, що передує навчальному року в системі «my.kpi.ua».

У разі неможливості формування навчальних груп для вивчення певної дисципліни студентам надається можливість здійснити повторний вибір, приєднавшись до вже сформованих навчальних груп (друга хвиля вибору). Результати вибору здобувачем навчальних дисциплін зазначаються в його індивідуальному навчальному плані в розділі «Обрані дисципліни» та засвідчуються його особистим підписом. Навчальні дисципліни, які внесені до індивідуального навчального плану здобувача, є обов'язковими для вивчення у відповідному семестрі.

Зверніть увагу: в анотаціях дисциплін Ф-каталогу вказуються викладачі, які попередньо плануються в якості лекторів відповідних дисциплін. Однак інколи можливі зміни, і лектор з обраної дисципліни не збігатиметься із зазначеним прізвищем!

**Перелік позначень**

Кафедри:

ММАД – кафедра математичного моделювання та аналізу даних
ММЗІ – кафедра математичних методів захисту інформації
ІБ – кафедра інформаційної безпеки
ПФ – кафедра прикладної фізики

| **Дисципліни для вибору на перший рік навчання** | | |
|---|---|---|
| Магістри першого курсу обирають **три** екзаменаційні дисципліни та **дві** залікові дисципліни з наведеного переліку для вивчення у **другому** семестрі | | |
| *Другий (весняний) семестр, екзаменаційні дисципліни* | | |
| *Дисципліна (5 кредитів, екзамен)* | *Кафедра* | *Стор.* |
| *Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах | ІБ | *5* |
| Методи аналізу великих гетерогенних даних | ММАД | *9* |
| Методи глибокого навчання на різнорідних даних | ММАД | *11* |
| *Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем | ІБ | *13* |
| *Теорія і методи соціальної інженерії в кібербезпеці | ІБ | *15* |
| Рефлексивний аналіз поведінки вибору | ІБ | *18* |
| Технологія блокчейн та розподілені системи | ММЗІ | *20* |
| Фізико-математичні основи квантової стеганографії | ІБ | *22* |
| Організаційне забезпечення оцінювання захищеності інформації | ІБ | *24* |
| Проектування комплексів захисту конфіденційної інформації | ІБ | *26* |
| Загальна теорія ігор | ММАД | *28* |

*Складові сертифікатної програми «Кібербезпека об’єктів критичної інфраструктури»

** для магістрів, які навчаються за дуальною програмою освіти з Samsung R&D Institute Україна.

Розробники Ф-каталогу

Прогонов Дмитро Олександрович  доцент, д.т.н., доцент кафедри ІБ

# ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

## (ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)

# Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах

## (Проф. Зубок В.Ю.)

| | |
|---|---|
| Сертифікатна програма | Кібербезпека об'єктів критичної інфраструктури |
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Практичних занять: 30 год<br>Самостійна робота студентів: 90 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | *Необхідно знати*: фізичну природу електромагнітних сигналів та середовища передачі даних, архітектуру комп'ютерних систем; операційні системи та їх безпеку; технології програмування; теорію інформації та кодування; нормативно правове забезпечення захисту інформації; методи та засоби забезпечення інформаційної безпеки; міжнародні та національні стандарти в сфері інформаційної безпеки.<br>*Необхідно вміти*: виконувати класифікацію автоматизованих систем; виконувати класифікацію інформації; виконувати аналіз профілю захищеності; визначати межі контрольованої зони; виконувати проектування та знати процедури забезпечення КСЗІ; виконувати класифікацію об'єктів інформаційної діяльності; розробляти політику безпеки для ОІД (об'єкт інформаційної діяльності); оцінювати ефективність мір захисту інформації. |
| Що буде вивчатися | Навчальна дисципліна «Захист інформації в спеціалізованих |

| | |
|---|---|
| | інформаційно-телекомунікаційних системах» присвячена окремим напрямкам та методам, які використовуються у напряму комплексного підходу до захисту інформаційних ресурсів на об’єктах інформаційної діяльності. Подається структурований матеріал, що відображає сучасні технології та моделі захисту інформації в телекомунікаційних системах та мережах. Докладно розглянуто основи захисту інформації та основні питання інформаційної безпеки національної мережі телекомунікацій, телекомунікаційних мереж загального користування та спеціального призначення, основні методи і засоби захисту телетрафіку, а також основи організації захисту інформації в галузі інформаційно-телекомунікаційних систем та їх мереж.<br>Основні теми, які розглядаються у курсі:<br>1. Системи та мережі передачі. Класифікація; загальні моделі та характеристики систем передачі інформації.<br>2. Моделі канал зв’язку. Поняття динамічного діапазону каналу зв’язку, узгодження характеристик.<br>3. Сучасні інформаційно-телекомунікаційні мережі. Класифікація мереж та середовища передачі даних, типи протоколів передачі даних в аспекті захисту інформаційних ресурсів та їх властивостей.<br>4. Інформаційно-телекомунікаційні системи та технології як об'єкти інформаційної безпеки.<br>5. Нормативно-правове забезпечення захисту інформації в інформаційно-телекомунікаційних системах та мережах згідно вітчизняних та світових вимог і стандартів.<br>6. Вимоги та критерії безпеки інформаційно-телекомунікаційних систем.<br>7. Управління інформаційними активами |

| | |
|---|---|
| | інформаційно-телекомунікаційних систем загального та спеціального призначення.<br>8. Моделі загроз та моделі порушника в інформаційно-телекомунікаційних системах та мережах.<br>9. Ризик менеджмент в інформаційно-телекомунікаційних системах загального та спеціального призначення.<br>10. Профілі захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах та мережах. Технології та архітектура управління забезпеченням.<br>Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал. |
| Чому це цікаво/треба вивчати | Навчальна дисципліна розглядає законодавчі вимоги до кіберзахисту спеціалізованих систем, нормативне забезпечення, міжнародні стандарти на кращі світові практики цієї діяльності, перш за все, в аспекті кібербезпеки так званих Операційних технологій (ICS/SCADA систем). Безпека операційних технологій, “Промисловості 4.0”, промислового Інтернету речей (IIoT) є одним з головних завдань кібербезпеки, особливо під час відновлення інфраструктури та промисловості України. |
| Чому можна навчитися | Сучасні технологічні тренди захисту інформації спеціалізованих ІКС. Загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих ІКС.<br>Спеціалізовані ІКС в державному та банківському секторі, в промисловості. Міжнародні документи з кіберзахисту промислових ІКС. Ключові аспекти спеціалізованих комунікаційних технологій в промисловості. Кіберінциденти в промисловості.<br>Огляд та архітектурно-функціональне порівняння відомих |

| | |
|---|---|
| | платформ та систем кіберзахисту спеціалізованих ІКС в промисловості. Архітектури та топології промислових ІКС. Порівняння вимог до безпеки загальних ІТ систем та ІКС управління технологічними процесами (АСУТП). Архітектура кіберзахисту спеціалізованих промислових ІКС. Сегментація, сегрегація, засоби впровадження. Заходи з забезпечення кібербезпеки в промисловості. Реагування на інциденти. Побудова політики безпеки спеціалізованої ІТС з використанням «контролів безпеки». |
| Як можна користуватися набутими знаннями та вміннями | Вивчення дисципліни дозволяє поглибити розуміння технологій та моделей захисту інформації в інформаційно-телекомунікаційних системах та мережах, їх властивостей, внутрішніх зв’язків та інтерпретацій у термінах різних дисциплін. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1oYhaM7ZS7vCQHO-JcPR-yJXs5cecCRWG?usp=sharing |
| Вид семестрового контролю | екзамен |

# Методи аналізу великих гетерогенних даних

**(Доцент Колотій А.В.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для вивчення дисципліни студент має бути знайомий з основами програмування, бажано на Python, структурами даних. Бажано розуміти принципи побудови та функціонування програмних систем, володіти навичками підготовки та аналізу даних, бути знайомим з методами штучного інтелекту, зокрема, нейронними мережами. |
| Що буде вивчатися | Технології розподіленої обробки даних, які можуть бути масштабовані для великих датасетів. Воркфлоу, які лежать в основі сучасних Data Warehouse. |
| Чому це цікаво/треба вивчати | Курс показує сучасні реалії підготовки та обробки великих різнорідних даних в розподілених системах |
| Чому можна навчитися | Розуміння основ роботи з інфраструктурою Apache Hadoop / Apache Spark. Створення воркфлоу для керування потоками даних в Data Warehouse. |

| | |
|---|---|
| Як можна користуватися набутими знаннями та вміннями | Для вирішення задач розподіленої обробки великих обсягів дани |
| Інформаційне забезпечення дисципліни | Силабус, Google Classrom з матеріалами https://drive.google.com/file/d/1prPUSfL_dTGyGTedy1rjooBdbSBiSig2/view?usp=sharing |
| Вид семестрового контролю | екзамен |

# Методи глибокого навчання на різнорідних даних

## (Асистент Яворський О.А.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Навички програмування на мові Python, знання з теорії ймовірності та математичної статистики, базові знання з машинного навчання, базові навички програмування на мові C++, базові знання з теорії оптимізації |
| Що буде вивчатися | - Основні архітектури глибинних мереж<br>- Методи fine-tuning (покращення) моделей<br>- Методи дистиляції знань<br>- Проблеми побудови RAG систем<br>- Фізично-обгрунтовані архітектури<br>- Проблеми оцінки якості та ефективності моделей<br>- Методи інженерії даних (feature engineering)<br>- Мультимодальні архітектури<br>- Вступ до роботи з CUDA |
| Чому це цікаво/треба вивчати | Атаки на основі соціальної інженерії складно піддаються виявленню технічними засобами, і є дуже поширеним та багатогранним явищем. Великий відсоток таких атак є успішним. |
| Чому можна навчитися | Дисципліна дозволить студентам краще ознайомитися з актуальними проблемами в глибинному навчанні, та |

| | |
|---|---|
| | оволодіти навиками, які необхідні для роботи з специфічними завданнями, а також такими, що вимагаються на спеціалізованих підприємствах |
| Як можна користуватися набутими знаннями та вміннями | - Навчання моделей<br>- Оцінка моделей<br>- Побудова застосунків, що базуються на глибинних даних<br>- Оптимізація існуючих моделей та застосунків |
| Інформаційне забезпечення дисципліни | Силабус, онлайн курси, курс в google classroom https://drive.google.com/file/d/1wYbZuWZe3k1UKRIgNUA0z-khT35cwnbh/view |
| Вид семестрового контролю | екзамен |

# Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

**(Доц. Барановський О.М.)**

| | |
|---|---|
| Сертифікатна програма | Кібербезпека об'єктів критичної інфраструктури |
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | Українська |
| Вимоги для початку вивчення дисципліни | Для успішного оволодіння матеріалом потрібно мати знання щодо методів захисту інформації в інформаційно — комунікаційних системах та підходів до захисту web-ресурсів. |
| Що буде вивчатися | Метою навчальної дисципліни є отримання знань та навичок про архітектуру, налаштування та супровід технологій захисту сучасних інформаційно-комунікаційних систем.<br>В процесі вивчення дисципліни розглядаються такі теми:<br>• Управління ідентифікаціями (Identity management)<br>• Системи контролю привілеїв користувачів (Privileged access management)<br>• Протоколи автентифікації та авторизації<br>• Засоби побудови віртуальних захищених мереж (VPN)<br>• Системи управління інформаційною безпекою та подіями безпеки (Security |

| | |
|---|---|
| | information and event management)<br>• Використання засобів віртуалізації та хмарних технологій для побудови захищених інформаційно-комунікаційних систем |
| Чому це цікаво/треба вивчати | Отримання знань та навичок щодо архітектури, налаштування та супроводу технологій захисту сучасних інформаційно-комунікаційних систем |
| Чому можна навчитися | В процесі вивчення дисципліни студенти засвоять такі теми:<br>• Управління ідентифікаціями (Identity management)<br>• Системи контролю привілеїв користувачів (Privileged access management)<br>• Протоколи автентифікації та авторизації<br>• Засоби побудови віртуальних захищених мереж (VPN)<br>• Системи управління інформаційною безпекою та подіями безпеки (Security information and event management)<br>• Використання засобів віртуалізації та хмарних технологій для побудови захищених інформаційно-комунікаційних систем |
| Як можна користуватися набутими знаннями та вміннями | В результаті вивчення навчальної дисципліни студенти зможуть застосувати отримані знання для аналізу захищеності інформаційно-комунікаційних систем, формування рекомендацій щодо підвищення ступеню їх захисту, а також роботи над обраними темами магістерських дисертацій |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1_zarwriqpQx7j4VWCVt4zzfXjp5j_cb1?usp=sharing |
| Вид семестрового контролю | екзамен |

# Теорія і методи соціальної інженерії в кібербезпеці

**(Доцент Стьопочкіна І.В.)**

| | |
|---|---|
| Сертифікатна програма | Кібербезпека об’єктів критичної інфраструктури |
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Практичних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Бажане уміння програмувати на мовах Java, Python. |
| Що буде вивчатися | Соціальна інженерія є одним із найуспішніших напрямків здійснення атак на об’єкти різного типу. Слабкою ланкою кожної системи захисту є людина, саме з участю людського фактору соціальний інженер досягає своєї мети. Уміння та знання, набуті в цьому курсі, можуть бути використані там, де передбачається діяльність із кіберзахисту інформації, в тому числі із використанням наукоємних технологій, на стику із методиками HR-менеджмента.<br>Навчальна дисципліна розглядає теоретичні основи відповідних атак. В тому числі, розглянуто моделі атак соціальної інженерії, моделі їх виявлення, сценарії різних видів атак соціальної інженерії, ПЗ, яке використовується при цьому та способи протидії цим атакам. Ці знання дають змогу зрозуміти фактори успіху відповідних атак, та попередити їх.<br>Теоретичні матеріали курсу дають студенту знання про: |

| | |
|---|---|
| | • Моделі та сценарії атак та їх виявлення;<br>• Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак;<br>• Механізми здійснення різних атак соціальної інженерії;<br>• Нові технології та засоби соціальної інженерії, засновані на ML та AI.<br>• Рішення кіберзахисту та підходи до попередження атак соціальної інженерії.<br>Також за дисципліною передбачено 5 комп'ютерних практикумів, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. |
| Чому це цікаво/треба вивчати | Атаки на основі соціальної інженерії складно піддаються виявленню технічними засобами, і є дуже поширеним та багатогранним явищем. Великий відсоток таких атак є успішним. Відповідно, проходження даного курсу дозволяє розширити знання студентів щодо ефективній протидії таким атакам. |
| Чому можна навчитися | Технікам соціальної інженерії (для задач offensive security), опанувати засоби та методи протидії. |
| Як можна користуватися набутими знаннями та вміннями | В результаті виконання практикумів студенти набувають такі уміння:<br>• Розробляти сценарії та моделі атак соціальної інженерії та здійснювати імітаційне моделювання;<br>• Уміння розробляти програму тестування на проникнення із використанням різних підходів;<br>• Використовувати наявні програмні засоби, за допомогою яких може діяти соціальний інженер, в цілях тестування на проникнення;<br>• Уміння розробляти методики |

| | |
|---|---|
| | оцінки персоналу на чутливість до різних атак соціальної інженерії;<br>• Уміння розробляти елементи засобів тестування на проникнення із використанням підходів соціальної інженерії.<br>За курсом передбачено модульну контрольну роботу для контролю засвоєння практичного та теоретичного матеріалу. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1bEgTKqgB95O4C0MY6UfZ96twY5CxMa0-?usp=sharing<br><br>Платформа “Сікорський”: курс «Теорія та методи соціальної інженерії в кібербезпеці» https://do.ipo.kpi.ua/course/view.php?id=1713 |
| Вид семестрового контролю | екзамен |

# Рефлексивний аналіз поведінки вибору

## (Доцент Смирнов С.А.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для розуміння змісту курсу студентам достатньо мати базові знання з основ математичного моделювання, дискретного аналізу та теорії імовірностей. |
| Що буде вивчатися | В курсі вивчаються особливості процесів прийняття рішень (ППР), пов’язані із рефлексивною структурою та станом свідомості людини, що приймає рішення. Завдання навчальної дисципліни — навчити студентів використовувати методи і прийоми моделювання поведінки вибору, аналізувати отримані моделі, визначати загрози та вразливості ППР, пов'язані з їх структурою та наповненням, а також з варіантами доступності інформації про це. |
| Чому це цікаво/треба вивчати | Моделі поведінки вибору, як одно- так і багатосуб’єктні, моделі рефлексивного керування на їх основі мають значну цінність в сучасних умовах, бо їх знання створюють можливості маніпуляції вибором (реклама, політтехнології, фішинг та соціальна інженерія), але також дозволяють знайти інструменти для захисту від таких маніпуляції. |

| | |
|---|---|
| Чому можна навчитися | Студенти зможуть використовувати методи і прийоми моделювання поведінки вибору, аналізувати отримані моделі, визначати загрози та вразливості ППР, пов'язані з їх структурою та наповненням, а також з варіантами доступності інформації про них. |
| Як можна користуватися набутими знаннями та вміннями | Отримані знання дозволяють моделювати та аналізувати рефлексивну структуру людської взаємодії, знаходити та блокувати загрози, спроби маніпуляції та рефлексивного керування. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1kZeQQ4YQGwkgll5Gxr1kNnX-BTMWvKb0?usp=sharing<br><br>Посилання на дистанційний ресурс:<br>Платформа “Сікорський”, курс “Рефлексивний аналіз поведінки вибору”<br>https://classroom.google.com/u/1/c/ODIyNTE2ODIzNjZa |
| Вид семестрового контролю | екзамен |

# Технологія блокчейн та розподілені системи

## (Проф. Кудін А.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 106 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Бажані знання щодо методів симетричної та асиметричної криптографії, сучасних криптосистем та протоколів |
| Що буде вивчатися | Навчальна дисципліна «Технології блокчейн та розподілені системи» присвячена сучасним криптографічним технологіям побудови розподілених баз даних із властивостями незмінюваності та спостережуваності; такі системи ґрунтуються на основі геш-ланцюгів блоків, більш відомих під назвою «блокчейн».<br>Теоретичний матеріал супроводжується комп'ютерними практикумами, на яких ви зможете самостійно розгорнути деякі блокчейн-системи та опанувати механізми їх роботи. |
| Чому це цікаво/треба вивчати | За результатами вивчення даного курсу студенти будуть ознайомлені з принципами функціонування новітніх blockchain-технологій, огляд сучасних протоколів консенсусу при формуванні геш-ланцюгів блоків. Це дозволить поглибити знання студентів щодо сучасних методів криптографічного захисту інформації. |
| Чому можна навчитися | У дисципліні буде розглянуто такі |

| | |
|---|---|
| | теми:<br>• «низова» структура блокчейнів;<br>• протоколи консенсусу: Proof of Work, Proof of Stake, Proof of Activity та ін.;<br>• децентралізовані та централізовані блокчейни (private ledgers);<br>• принципи роботи криптовалют та смарт-контрактів. |
| Як можна користуватися набутими знаннями та вміннями | Отримані знання дозволяють проводити аналіз та практично використовувати blockchain-технології для побудови розподілених баз даних із властивостями незмінюваності та спостережуваності |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1dsXa76wYk9R5qbs1Sb6z8gvANb7KrNdr?usp=sharing |
| Вид семестрового контролю | екзамен |

# Фізико-математичні основи квантової стеганографіїі

**(професор, д.т.н. Мачуський Є.А., доцент, д.т.н., Прогонов Д.О.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмеження |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 16 год<br>Самостійна робота студентів: 104 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | ● знання основ математичного аналізу;<br>● знання основ спектрального аналізу сигналів;<br>● знання пакетів для моделювання на мові програмування Python;<br>знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості). |
| Що буде вивчатися | Метою навчальної дисципліни є розширення у студентів компетентностей з розуміння фізико-математичних основ квантової стеганографії. Предметом дисципліни є методи квантової стеганографії та стегоаналізу. |
| Чому це цікаво/треба вивчати | За результатами вивчення дисципліни проводиться поглиблення розуміння основ побудови та застосування методів квантової стеганографії, а також сучасних тенденцій розвитку в даній галузі. |
| Чому можна навчитися | ● Знання термінології в галузі цифрової та квантової стеганографії й стегоаналізу<br>● Вміння практичного застосування стеганографічних методів обробки даних, зокрема особливостей |

| | |
|---|---|
| | використання методів квантової стеганографіїї<br>● Поглиблення навичок практичного застосування методів стегоаналізу даних<br>● Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних. |
| Як можна користуватися набутими знаннями та вміннями | Побудова статистичних моделей та методів виявлення стеганограм, сформованих на основі цифрових даних. Оцінка якості роботи методів квантової стеганографії. |
| Інформаційне забезпечення дисципліни | Посилання на силабус:<br><br>https://drive.google.com/drive/folders/1NjzPAxnku7W_3KdXL-CPjeaArudZdk0c?usp=sharing |
| Вид семестрового контролю | екзамен |

# Організаційне забезпечення оцінювання захищеності інформації

**(Ст. викладач, д.т.н. Морщ Є.В.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Практичних занять: 16 год<br>Самостійна робота студентів: 104 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Необхідні знання, навички та вміння в області компонентної бази пристроїв ТЗІ, а також правових основ захисту інформації. |
| Що буде вивчатися | Метою дисципліни є вивчення порядку організації та проведення державної експертизи у сфері технічного захисту інформації, принципів державної політики у сфері ліцензування, ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації, питань нагляду і контролю у сфері ліцензування. |
| Чому це цікаво/треба вивчати | Ознайомлення з сучасним станом нормативної документації в галузі технічного захисту інформації, розуміння принципів державної політики у сфері ліцензування |
| Чому можна навчитися | За результатами вивчення курсу здобувачі отримають навички практичної роботи з технічних регламентів і передбачених ними процедур оцінки відповідності, а також здійсненням добровільної оцінки відповідності, організацією стандартизації в Україні |

| | |
|---|---|
| Як можна користуватися набутими знаннями та вміннями | Під час вивчення дисципліни проводиться ознайомлення з організаційними засадами розроблення, прийняття та застосування технічних регламентів і передбачених ними процедур оцінки відповідності, а також здійсненням добровільної оцінки відповідності, організацією стандартизації в Україні. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1sOY4Uk2Xw3hc4qhz1PhATRLesH78mO0j?usp=sharing |
| Вид семестрового контролю | екзамен |

# Проектування комплексів захисту конфіденційної інформації

**(доцент, к.т.н. Луценко В.М.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 16 год<br>Самостійна робота студентів: 104 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для освоєння курсу студенти повинні мати тверді знання щодо основ програмування, теорії кіл та обробки сигналів, компонентної бази та схемотехніки пристроїв ТЗІ, основи роботи з технічною документацією та протоколами міжнародних стандартів техніки ТЗІ. |
| Що буде вивчатися | Курс присвячений проектуванню та створенню засобів технічного захисту інформації від несанкціонованого доступу та проектуванню комплексних системи захисту інформації. В основу курсу покладено нормативні документи та рекомендації з технічного захисту інформації, а також світові стандарти. |
| Чому це цікаво/треба вивчати | Розуміння принципів проектуванню та створенню засобів технічного захисту інформації від несанкціонованого доступу та проектуванню комплексних системи захисту інформації. Ознайомлення з нормативними документами та рекомендаціями з технічного захисту інформації. |
| Чому можна навчитися | За результатами вивчення курсу студенти отримають навички щодо підготовки та проведення проектуванню |

| | |
|---|---|
| | комплексних системи захисту інформації. |
| Як можна користуватися набутими знаннями та вміннями | За результатами навчання студенти отримують практичні навички з проектування комплексних систем захисту інформації та проведення державної експертизи у сфері технічного захисту інформації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1sNcZ-zNJb87AMrIZXuAOhiAtBVI0Qlo6?usp=sharing |
| Вид семестрового контролю | екзамен |

# Загальна теорія ігор

**(Доц. Терещенко І.М.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Практичнихзанять: 16 год<br>Самостійна робота студентів: 104 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для розуміння змісту курсу студентам достатньо мати базові знання з наступних навчальних дисциплін: математичне моделювання, дискретний аналіз, теорія ймовірностей. |
| Що буде вивчатися | В курсі вивчаються особливості процесів прийняття рішень, пов’язані із структурою конфліктної взаємодії, можливостями щодо впливу та оцінювання результатів з боку сторін, що приймають рішення. |
| Чому це цікаво/треба вивчати | Навчальна дисципліна «Загальна теорія ігор» присвячена формуванню у студентів здатності застосовувати спеціальні математичні поняття, означення, алгоритми та методи, що необхідні для вивчення наступних спеціальних дисциплін, вивчення найважливіших професійно корисних результатів прикладної математики. |
| Чому можна навчитися | Завдання навчальної дисципліни — навчити студентів використовувати математичні методи теорії ігор для розв’язання різноманітних прикладних задач прикладного характеру, пов’язаних з оптимізацією функцій, які виникають у практичної діяльності. |
| Як можна користуватися набутими знаннями та вміннями | В результаті навчання студент набуває такі уміння:<br>- уміння формалізувати задачу, в межах термінів теорії ігор формулювати її математичну постановку;<br>- уміння зводити матричну гру до задачі лінійного програмування;<br>- уміння застосовувати графо-аналітичний метод; |

| | |
|---|---|
| | - уміння знаходити рішення гри за допомогою домінуючих стратегій;<br>- уміння знаходити арбітражне рішення Неша;<br>- уміння застосовувати кооперативні ігри, створювати коаліції;<br>- уміння знаходити поділ за допомогою С-ядра або вектора Шеплі.<br>Ці уміння необхідні для розуміння та використання загальних зв'язків між вивченими математичними поняттями і методами та актуальними практичними задачами. |
| Інформаційне забезпечення дисципліни | - Посилання на силабус: https://drive.google.com/file/d/18Z_SSCo8hhYHJ30cgwzMmFa4qiLNBrsJ/view?usp=sharing<br>Посилання на дистанційний ресурс:<br>Платформа "Сікорський", курс "Загальна теорія ігор"<br>https://classroom.google.com/c/MTQyNDc1MjgwOTg2 |
| Вид семестрового контролю | екзамен |

# Моделі та методи криптоаналізу блокових шифрів

**(Доц. Яковлев С.В.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичних методів захисту інформації |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **5 кредити ЄКТС, 150 год**<br>Лекційних занять: 30 год<br>Практичних занять: 16 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 90 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Базові знания з наступних дисциплін: теорія ймовірності, симетрична криптографія, математична статистика, методи криптоаналізу |
| Що буде вивчатися | Основною метою дисципліни є формування у студентів глибинного розуміння сучасних статистичних методів криптоаналізу.<br><br>У дисципліні будуть детально розглянуті такі теми: 1) будова ітеративних шифрів, схеми блокового шифрування; 2) статистичні атаки на раундові ключі; 3) формальна теорія диференціального криптоаналізу, теоретична (доказова) та практична стійкість шифрів до диференціального криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість; 4) модифікаці'і та узагальнення диференціального криптоаналізу: аналіз неможливих диференціалів, аналіз диференціалів вищого порядку, атаки бумерангів та прямокутників, атаки на пов'язаних ключах; 5) формальна теорія лінійного криптоаналізу, теоретична (доказова) та |

| | |
|---|---|
| | практична стійкість шифрів до лінійного криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість; 6) модифікаці'і та узагальнення лінійного криптоаналізу: білінійний криптоаналіз, узагальнений лінійний криптоаналіз на довільних абелевих групах, аналіз нульових кореляцій, диференціально- лінійні розпізнавачі; 7) методи автоматизованого пошуку високоймовірних та неможливих диференціалів, високймовірних лінійних апроксимацій; 8) інтегральний криптоаналіз та йога узагальнення: аналіз лінійних підпросторів, властивості подільності. |
| Чому це цікаво/треба вивчати | Багато сучасних інформаційних систем використовують блокові шифри, зокрема AES та DES. Для успішного аналізу рівня захищеності та пошуку вразливостей таких систем, необхідно знати відповідні криптографічні властивості блокових шифрів та вміти здійснювати 'іх криптоаналіз. |
| Чому можна навчитися | Студенти отримують знания моделей та методів криптоаналізу блокових шифрів, параметрів стійкості до криптоаналітичних атак та 'іх поведінку; вміння будувати статистичні атаки на ітеративні блокові шифри та одержувати аналітичні чи розрахункові оцінки стійкості до таких атак. |
| Як можна користуватися набутими знаннями та вміннями | Створювати та аналізувати сучасні методи блокового шифрування, оцінювати та контролювати гарантований рівень захисту при шифруванні. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/luUogeDExAda2Wsvs7BJo7K0gt1EjzmBY?usp=sharing |
| Вид семестрового контролю | екзамен |

# ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

## (ЗАЛІКОВІ ДИСЦИПЛІНИ)

# Web - аналітика

## (Доц. Ткач В.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **4 кредити ЄКТС, 120 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 76 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Предмет базується на знаннях в галузі програмного забезпечення ЕОМ, програмування та створення web-застосунків. |
| Що буде вивчатися | Сучасний розвиток світових комунікацій, зокрема всесвітньої мережі Інтернет, а також велика кількість інформаційних ресурсів, що в ній представлено, зумовлюють необхідність досконалого вивчення інформаційних потоків, аналізу джерел інформації, кількісних та якісних характеристик.<br>Сучасний рівень розвитку інформаційних технологій вимагає широкого спектру практичних навичок роботи з застосуванням різних методологій програмування.<br>Програмування є лише інструментом для вирішення практичних та науково-практичних задач. Така підготовка може забезпечити можливість пристосування до нових типів задач, пов’язаних з використанням у тому числі високопродуктивної обчислювальної техніки.<br>Дослідник повинен володіти технологіями програмування, достатніми для отримання та обробки відкритих даних з мережі Інтернет, з систем збору аналітики з їх подальшим використанням |

| | |
|---|---|
| | для розв’язання складних ресурсоємних наукових задач, що як правило мають міждисциплінарний характер. |
| Чому це цікаво/треба вивчати | Ознайомлення з принципами пошуку аномалій в даних веб-аналітики, основами поведінкового аналізу користувачів в мережі Інтернет |
| Чому можна навчитися | В межах дисципліни розглянуто основні принципи аналізу даних, що збираються в Інтернет, принципи пошуку аномалій в даних веб-аналітики, принципи визначення нормальної та аномальної поведінки користувачів в мережі Інтернет і т.д. |
| Як можна користуватися набутими знаннями та вміннями | Отримані знання можуть використовуватися при підготовці магістерської дисертації, зокрема аналізу даних, що збираються в Інтернет, принципи пошуку аномалій в даних веб-аналітики |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1TGbOCpNYMUGSSk64N8LSX4aHISBNLEDV?usp=sharing |
| Вид семестрового контролю | залік |

# Проектування розподілених систем

## (Доцент Родіонов А.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмеження |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **4 кредити ЄКТС, 120 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 76 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | • Знання архітектури та принципів розробки ПЗ, бази даних, мережева взаємодія та протоколи прикладного рівня.<br>• Знання будь-якої мови програмування та створення за її допомогою Web-застосувань |
| Що буде вивчатися | Навчальна дисципліна присвячена теоретичним та практичним аспектам створення масштабованих, високонавантажених та високодоступних розподілених систем, а також програмного забезпечення на їх основі.<br>Практичні завдання присвячені розробці невеликих застосувань на основі шаблонів мікросервісів. У груповому проекті необхідно реалізувати розподілене та відмовостійке застосування на основі мікросервісної архітектури. |
| Чому це цікаво/треба вивчати | У курсі розглядається базова теорія пов’язана з розподіленими системами і велика частина курсу присвячена мікросервісній архітектурі та шаблонам мікросерівів. |
| Чому можна навчитися | Основні теми курсу:<br>• Масштабованість, продуктивність, доступність сучасних застосувань |

| | |
|---|---|
| | • Шаблони зв'язку в розподілених системах: RPC, Async, Messaging, gRPC<br>• Проблеми комунікації повідомленнями: Duplicate, Delay, Drop, Reorder<br>• Distributed systems: Communication, Failure Modes, Leader, Consensus, Quorums, Time, Order<br>• Монолітна та мікросервісна архітектура - переваги та недоліки<br>• Шаблони мікросервісної архітектури: Service Discovery & Service Registry, Deployment Strategy, Microservice chassis, Distributed tracing, DB per service, API Gateway, Circuit Breaker, Testing, Backpressure<br>• Розподілені транзакції<br>• Системи обміну повідомленнями<br>• Архітектура на основі обміну повідомленнями |
| Як можна користуватися набутими знаннями та вміннями | Отримані знання та навички можуть використовуватися для реалізації розподілених та відмовостійких високонавантажених систем, зокрема із застосуванням мікросервісної архітектури. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1WjA1CoO6UZC2nPrLK5GhGlkMxHLUwIkt?usp=sharing |
| Вид семестрового контролю | залік |

# Рішення в умовах невизначеності та ризику

**(Доцент Смирнов С.А.)**

| | |
|---|---|
| Сертифікатна програма | Кібербезпека об’єктів критичної інфраструктури |
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмеження |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **4 кредити ЄКТС, 120 год**<br>Лекційних занять: 30 год<br>Лабораторних занять: 14 год<br>Самостійна робота студентів: 76 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для успішного засвоєння курсу потрібні базові знання з математичного аналізу, алгебри і геометрії, дискретного аналізу, математичного моделювання. |
| Що буде вивчатися | Метою курсу є вивчення теоретичних основ та практичних методів прийняття рішень в умовах невизначеностей різної природи: множинної, ймовірністної, конфліктної. Обговорюються також методи контролю та подолання різних форм складності, ризику та невизначеності, що містяться в практичних ситуаціях прийняття рішень. |
| Чому це цікаво/треба вивчати | Викладаються математичні засоби що дозволяють успішно долати шлях від неформалізованої постановки задачі з боку Замовника, через проактивне моделювання ситуації, до варіантів її точного розв’язання Виконавцем. |
| Чому можна навчитися | Розв’язувати задачі оцінювання та прийняття рішень в умовах невизначеності та ризику від виникнення проблеми до отримання результату |
| Як можна користуватися набутими | Набуті знання та вміння щодо |

| | |
|---|---|
| знаннями та вміннями | сучасних методів підтримки прийняття рішень в умовах невизначеності можуть бути використані для розв'язання широкого кола задач за темою магістерської дисертації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/14Q8h3tj3SPojyXIVIZtb9SWGap_2_OIN?usp=sharing<br>Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Рішення в умовах невизначеності та ризику" https://classroom.google.com/u/1/c/OTk3MTgyNzQzNDNa?hl=uk |
| Вид семестрового контролю | залік |

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ**

**(Професор Шелестов А.Ю.)**

| | |
|---|---|
| Сертифікатна програма | Моделі та методи інтелектуального аналізу гетерогенних даних |
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | Другий ( магістерський) |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **Загальна кількість: (4 кредити ЄКТС) 120 год**<br>Лекційних занять: 30 год<br>Практичних занять: 14 год<br>Самостійна робота студентів: 76 год |
| Мова викладання | Українська |
| Вимоги для початку вивчення дисципліни | Студент має бути знайомий з основами програмування, бажано на Python, структурами даних, проте досвід проектування алгоритмів необов'язковий. Бажано також розуміти загальні принципи побудови та функціонування програмних систем. |
| Що буде вивчатися | Технології аналізу великих різнорідних даних |
| Чому це цікаво/треба вивчати | Наразі дані великого об’єму аналізуються та обробляються великою кількістю систем. Одним з сучасних підходів до розв’язання таких задач на основі великих даних є використання хмарних інфраструктур, які дозволяють використовувати набір віддалених обчислювальних компонентів для обробки даних як одну з інформаційних підсистем. Саме вивченню таких технологічних рішень і присвячено даний освітній компонент. |
| Чому можна навчитися | Володінню методами та засобами аналізу великих гетерогенних даних |
| Як можна користуватися набутими знаннями та вміннями | Знання та вміння, набуті в процесі вивчення дисципліни "Інформаційні технології аналізу великих гетерогенних даних" дозволять використовувати сучасні інструменти побудови розподілених додатків та використовувати хмарні ресурси для розв’язання прикладних задач на мультимодальних даних. |
| Інформаційне забезпечення дисципліни | Силабус, монографія, навчальний посібник |
| Вид семестрового контролю | Залік |

## Захист конфіденційної інформації з використанням методів машинного навчання

**(доцент, д.т.н. Прогонов Д.О.)**

| | |
|---|---|
| Сертифікатна програма | Кібербезпека об’єктів критичної інфраструктури |
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Можливі обмеження | Без обмежень |
| Можливі обмеження | Без обмежень |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **4 кредити ЄКТС, 120 год**<br>Лекційних занять: 30 год<br>Практичних занять: 30 год<br>Самостійна робота студентів: 60 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | • знання основ математичного аналізу;<br>• знання основ спектрального аналізу сигналів;<br>• знання пакетів для моделювання на мові програмування Python;<br>• знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості). |
| Що буде вивчатися | Метою навчальної дисципліни є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації з обмеженим доступом в умовах опрацювання значних об’ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних. |
| Чому це цікаво/треба вивчати | Поглиблення розуміння принципів роботи, області застосування та обмежень сучасних статистичних моделей даних. Підвищення точності |

| | |
|---|---|
| | роботи статистичних моделей в умовах зашумленості та/або даних. |
| Чому можна навчитися | ● Знання термінології в галузі аналізу та класифікації (кластеризації) даних;<br>● Знання методів моделювання багатовимірних сигналів в умовах обмеженості або відсутності даних щодо їх статистичних характеристик;<br>● Знання поширених методів класифікації (кластеризації) багатовимірних даних;<br>● Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних.<br>● Вміння вибору статистичних моделей багатовимірних сигналів з врахуванням наявної інформації щодо їх статистичних та кореляційних характеристик;<br>● Вміння застосування методів класифікації (кластеризації) даних в умовах обробки реальних (зашумлених) сигналів;<br>● Вміння проведення оцінювання якості роботи систем класифікації (кластеризації) даних; |
| Як можна користуватися набутими знаннями та вміннями | Отримані знання та вміння можуть бути використаними для вирішення практичних завдань, пов’язаних із застосуванням методів теорії розпізнавання образів для обробки різнорідних типів даних. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1q7TbM-IOiLp0MBJ7FLFxAX4xySa_zQ0q?usp=sharing |
| Вид семестрового контролю | залік |

# ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 1

| | |
|---|---|
| Лектор | Доцент Прогонов Д.О. |
| Кафедра, яка забезпечує викладання | Інформаційної безпеки |
| Рівень вищої освіти | Другий (магістерський) |
| Можливі обмеження | Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **Загальна кількість: (4 кредити ЄКТС) 120 год**<br>Лекційних занять: 0 год<br>Лабораторних занять: 0 год<br>Самостійна робота студентів: 120 год |
| Мова викладання | Українська |
| Вимоги до початку вивчення дисципліни | Прослухані курси «Математичний аналіз», «Програмування»<br>Рекомендовані знання:<br>- Основ спектрального аналізу сигналів<br>- Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python<br>- Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості) |
| Що буде вивчатися | Метою навчальної дисципліни є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації з обмеженим доступом в умовах опрацювання значних об'ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних. |
| Чому це цікаво/треба вивчати | Оволодіння знаннями і навичками даної дисципліни озброює студента поглибленими компетенціями в сучасних інформаційних технологіях |
| Чому можна навчитися | Поглиблення розуміння принципів роботи, області застосування та обмежень сучасних статистичних моделей даних. Підвищення точності роботи статистичних моделей в умовах зашумленості та/або даних. |
| Як можна користуватися набутими знаннями і уміннями | Отримані знання та вміння можуть бути використаними для вирішення практичних завдань, пов'язаних із застосуванням методів теорії розпізнавання образів для обробки різнорідних типів даних. |
| Інформаційне забезпечення дисципліни | Силабус |

| | |
|---|---|
| Вид семестрового контролю | Залік |

## ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 1

| | |
|---|---|
| Лектор | Доцент Прогонов Д.О. |
| Кафедра, яка забезпечує викладання | Інформаційної безпеки |
| Рівень вищої освіти | Другий (магістерський) |
| Можливі обмеження | Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **Загальна кількість: (4 кредити ЄКТС) 120 год**<br>Лекційних занять: 0 год<br>Лабораторних занять: 0 год<br>Самостійна робота студентів: 120 год |
| Мова викладання | Українська |
| Вимоги до початку вивчення дисципліни | Прослухані курси «Математичний аналіз», «Програмування»<br>Рекомендовані знання:<br>- Основ спектрального аналізу сигналів<br>- Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python<br>- Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості) |
| Що буде вивчатися | Метою навчальної дисципліни є формування у студентів компетентностей з проведення порівняльного аналізу сучасних пристроїв, систем та комплексів захисту інформації за наявною у відкритому доступі інформацією, роботи з науковою літературою для визначення альтернативних (конкуруючих) рішень та/або методів вирішення задач обробки та захисту інформації. Предметом дисципліни є методи аналізу систем. |
| Чому це цікаво/треба вивчати | Поглиблення розуміння методів імітаційного моделювання складних систем. |
| Чому можна навчитися | Знання методів декомпозиції та порівняльного аналізу складних систем;<br>Знання методів проведення імітаційного моделювання елементів та систем обробки даних;<br>Вміння проведення наукового пошуку альтернативних (конкуруючих) рішень та/або методів вирішення задач обробки та захисту інформації;<br>Навички практичної роботи з сучасними системами комп'ютерно математики для проведення імітаційного моделювання (MATLAB Simulink, LabVIEW, Wolfram System Modeler, Modelica). |
| Як можна користуватися набутими знаннями і уміннями | Підвищення точності імітаційного моделювання фізичних процесів та явищ. |
| Інформаційне забезпечення дисципліни | Силабус |
| Вид семестрового контролю | Залік |

## ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

| | |
|---|---|
| Кафедра | Математичних методів захисту інформації |
| Рівень вищої освіти | Другий ( магістерський) |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин | **Загальна кількість: 4 кредити ЄКТС, 120 годин**<br>Лекційних занять: 30 год<br>Самостійна робота студентів: 90 год |
| Мова викладання | Українська |
| Вимоги до початку вивчення дисципліни | Пройдений курс «Криптографія» або знання основних положень симетричної та асиметричної криптографії (поняття ключа, шифру, цифрового підпису, основних сучасних алгоритмів шифрування та цифрового підпису) |
| Що буде вивчатися | Основні теми, які розглядаються у курсі:<br>0) електронні довірчі послуги, класифікація електронних підписів та їх функціональність; механізми eIDAS;<br>1) життєвий цикл криптографічних ключів, організація керування життєвим циклом ключів, різні варіанти будови інфраструктур відкритих ключів, Центри сертифікації ключів;<br>2) мова ASN.1, стандарти кодування BER, CER, DER;<br>3) формат сертифікатів відкритих ключів X.509v3;<br>4) перевірка статусу сертифікатів, атрибутні сертифікати, списки відкликаних сертифікатів, протокол OCSP;<br>5) протоколи керування сертифікатами (PKCS10, CMC, CMP);<br>6) формати криптографічних повідомлень (CMS), підписані повідомлення, часові штемпелі; розширені формати підписаних повідомлень (CAdES);<br>7) формати захищених повідомлень. |
| Чому це цікаво/треба вивчати | Навчальна дисципліна «Інфраструктури відкритих ключів» знайомить студентів з принципами, методами та механізмами організації систем керування ключами та захищеного документообігу. Такі системи зараз надзвичайно поширені через невпинну та невблаганну діджиталізацію послуг та сервісів, впровадження якої вимагає відповідних механізмів безпеки (зокрема, захисту персональних даних) |
| Чому можна навчитися | Після опанування курсу студенти знатимуть основні принципи роботи центрів сертифікації ключів, організації життєвого циклу ключів, форматів основних структур даних, які використовуються у механізмах захисту систем захищеного документообігу |
| Як можна користуватися набутими знаннями і уміннями | Одержані знання та навички дозволяють користуватись на практиці системами, які використовують кваліфікований електронний підпис, та системами захищеного документообороту, самостійно розробляти, проектувати, впроваджувати та інтегрувати системи криптографічного захисту з урахуванням нормативно-правових аспектів, пов’язаних із використанням цифрових підписів. |
| Інформаційне забезпечення дисципліни | Силабус:<br>https://mmis.ipt.kpi.ua/education/education-master-syllabi/ |
| Вид семестрового контролю | Залік |

# Теорія захисту інформаційних ресурсів обмеженого доступу

**(доц., д.т.н. Прогонов Д.О.)**

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | **4 кредити ЄКТС, 120 год**<br>Лекційних занять: 30 год<br>Практичних занять: 14 год<br>Самостійна робота студентів: 76 год |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для освоєння курсу студенти повинні мати тверді знання щодо основ електродинаміки, компонентної бази ТЗІ, а також проектування систем ТЗІ |
| Що буде вивчатися | Метою курсу є вивчення базових понять та принципів функціонування пристроїв з точки зору можливості утворення каналів витоку інформації за рахунок ПЕМВН, протидії НСД до ІзОД електричними та електромагнітними каналами, у тому числі, віброакустичних, а також ознайомлення з їх проектуванням та конструюванням на прикладах найбільш поширених пристроїв. |
| Чому це цікаво/треба вивчати | Даний курс дозволяє поглибити знання в частині фахової підготовки з технічного захисту інформації разом з дисциплінами «ТЗІ», «ЗІ в телекомунікаційних системах», «Радіопротидія», «Проектування СЗІ» та ін. |
| Чому можна навчитися | Ознайомлення з базовими принципами утворення каналів витоку інформації за рахунок ПЕМВН, протидії НСД до ІзОД електричними та електромагнітними каналами. Отримання навичок щодо проектуванням та конструюванням найбільш поширених пристроїв з технічного захисту інформації. |
| Як можна користуватися набутими знаннями та вміннями | Увага приділяється питанням, що складають зміст проблематики технічного захисту інформації (ЗІ), а саме, нелінійним перетворенням, каналам побічних випромінювань та рівням захищеності від завад. |

| | |
|---|---|
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1HBCHauz36b9d1eb_c2NxIk6Ngls0UQ8L?usp=sharing |
| Вид семестрового контролю | залік |