НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від « 2 » червня 2023 р.)

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

**для здобувачів ступеня магістра за освітньою програмою**
**«Системи, технології та математичні методи кібербезпеки»,**
**за спеціальністю 125 Кібербезпека та захист інформації**

УХВАЛЕНО:

Вченою радою ФТІ
КПІ ім. Ігоря Сікорського
(протокол №7 від «15» травня 2023 р.)

Київ – 2023

Процедура вибору освітніх компонент відбувається згідно «Положення про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/node/185)

Силабуси усіх дисциплін та інша супровідна інформація розміщена на сайті кафедри: http://is.ipt.kpi.ua/is/individualnij-vibir-distsiplin-za-osvitnoyu-programoyu/

| **Дисципліни для вибору на перший рік навчання** | | |
|---|---|---|
| Студенти першого курсу магістратури (ОПП і ОНП) 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.* |
| 1 Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах | ІБ | *4* |
| 2 Основи теорії ідентифікації систем | ІБ | *7* |
| 3 Методи аналізу великих гетерогенних даних | ММАД | *9* |
| 4 Методи глибокого навчання на різнорідних даних | ММАД | *10* |
| 5 Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем | ІБ | *11* |
| 6 Теорія і методи соціальної інженерії в кібербезпеці | ІБ | *13* |
| 7 Рефлексивний аналіз поведінки вибору | ІБ | *14* |
| 8 Технологія блокчейн та розподілені системи | ММЗІ | *15* |
| 9 Моделі та методи криптоаналізу блокових шифрів | ММЗІ | *17* |
| ***Другий (весняний) семестр, залікові дисципліни*** | | |
| ***Дисципліна (4 кредити, залік)*** | | |
| 10 Web - аналітика | ІБ | *20* |
| 11 Проектування розподілених систем | ІБ | *22* |
| 12 Рішення в умовах невизначеності та ризику | ІБ | *24* |
| 13 Інформаційні технології аналізу великих гетерогенних даних | ММАД | *25* |
| 14 Інфраструктури відкритих ключів | ММЗІ | *26* |
| 15 Проактивний захист персональних даних 1* | ІБ | *28* |
| 16 Проактивний захист персональних даних 2* | ІБ | *29* |

| **Дисципліни для вибору на другий рік навчання** | | |
|---|---|---|
| Студенти першого курсу магістратури (ОНП) обирають **дві** залікові дисципліни з наведеного переліку для вивчення у **третьому** семестрі другого курсу | | |
| *Третій (осінній) семестр, залікові дисципліни* | | |
| *Дисципліна (4 кредити, залік)* | | |
| 17 Безпека кіберфізичних систем | ІБ | *32* |
| 18 Методи реалізації криптографічних механізмів | ММЗІ | *34* |
| 19 Моделі цінності інформації та ефективність інформаційного захисту | ММЗІ | *36* |
| 20 Моделювання складних систем | ІБ | *38* |
| 21 *Технології штучного інтелекту у системах інформаційної безпеки | ІБ | *40* |
| 22 *Технології захисту персональних даних | ІБ | *42* |

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

**Перелік позначень**

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

# ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

## (ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)

# 1. ЗАХИСТ ІНФОРМАЦІЇ В СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

(проф. Зубок В.Ю.)

| | |
|---|---|
| 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 | 5 кредитів ECTS |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Необхідні знання з основи технологій захисту інформації, бажано володіння основами теорії ризиків. |
| Що буде вивчатися | – класифікація інформаційно-комунікаційних систем за вимогами інформаційної безпеки відповідно до призначення цих систем;<br>– нормативно-правове та законодавче регулювання питань кібербезпеки в спеціалізованих ІКС;<br>– міжнародні документи з питань кібербезпеки спеціалізованих ІКС, зокрема на об'єктах критичної інфраструктури та в промисловості;<br>– моделі та сценарії атак на промислові спеціалізовані ІКС та їх виявлення;<br>– механізми здійснення різних атак на промислові спеціалізовані ІКС;<br>– архітектуру кіберзахисту та сучасні комплексні засоби кіберзахисту спеціалізованих ІКС в промисловості;<br>– заходи з забезпечення кібербезпеки спеціалізованих ІТС в промисловості. |
| Чому це цікаво/треба вивчати | Навчальна дисципліна розглядає законодавчі вимоги до кіберзахисту таких 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.<br>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 | Основною метою дисципліни є поглиблення у студентів розуміння загальних напрямів технічної політики з забезпечення кібербезпеки спеціалізованих ІКС, ключових аспектів спеціалізованих комунікаційних технологій в промисловості, дослідження актуальних кіберзагроз, сценарії відомих кіберінцидентів, провідних платформ та систем кіберзахисту для операційних технологій. Ці знання дають змогу формулювати політики безпеки спеціалізованих ІКС, розуміти основні засоби реалізації цієї політики та контролювання її виконання з урахуванням законодавчих вимог. |
| Інформаційне забезпечення дисципліни | Посилання на силабус:<br>https://drive.google.com/drive/folders/1O2ee0PB40oDhTX6ALKFWSnCfSnCwaBtj?usp=sharing<br><br>Матеріали дисципліни публікуються на платформі Sikorsky Google Workspace. Код курсу (2023) g66u6ik |
| Вид семестрового контролю | екзамен |

# 2. ОСНОВИ ТЕОРІЇ ІДЕНТИФІКАЦІЇ СИСТЕМ

(проф. Мачуський Є.А.)

| | |
|---|---|
| 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 | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | – знання основ математичного аналізу;<br>– знання основ спектрального аналізу сигналів;<br>– знання сучасних систем комп'ютерної математики та 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 «Основи теорії ідентифікації систем» є формування у студентів компетентностей з розробки математичних моделей динамічних систем для вирішення задачі визначення (ідентифікації) невідомих систем за частковими даними. Предметом дисципліни є методи статистичного моделювання динамічних систем. |
| Чому це цікаво/треба вивчати | Поглиблення розуміння сучасних підходів до ідентифікації систем обробки даних за наявними (частковими) даними. Розуміння методів непрямого визначення параметрів системи обробки даних. |
| Чому можна навчитися | – Знання термінології в галузі моделювання динамічних систем;<br>– Знання методів моделювання динамічних систем за відомими даними;<br>– Знання підходів до ідентифікації динамічних систем за повними або частковими даними;<br>– Вміння вибору підходів до розробки математичних моделей динамічних систем;<br>– Вміння застосування методів підпросторів та похибки передбачення в задачах ідентифікації систем;<br>– Вміння проведення оцінювання точності розробленої математичної моделі динамічної системи; |

| | |
|---|---|
| | – Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних. |
| Як можна користуватися набутими знаннями та вміннями | Побудова статистичних моделей та методів визначення параметрів систем обробки сигналів за наявними даними. Оцінка якості роботи даних моделей та методів. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1QtdFG_qjVeE0j96wGxs5gQC0fzfyaSI6?usp=sharing<br><br>–Murphy Kevin P. Machine Learning: A Probabilistic Perspective. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2012. – 1104 p. – ISBN 978-0262018029.<br>–Bishop Christopher M. Pattern Recognition and Machine Learning. – Information Science and Statistics series. – Springer, 2011. – 738 p. – ISBN 978-0387310732. |
| Вид семестрового контролю | екзамен |

# 3. МЕТОДИ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ

(проф. Шелестов А.Ю.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для вивчення дисципліни студент має бути знайомий з основами програмування, бажано на Python, структурами даних, проте досвід проектування алгоритмів або участі в олімпіадах необов'язковий. 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 | Дисципліна "Методи аналізу великих гетерогенних даних" присвячена вивченню теоретичних положень і сучасних методів математичного моделювання, аналізу та обробки гетерогенних даних, методів регресійного аналізу та кластеризації, нейронних мереж тощо. |
| Чому це цікаво/треба вивчати | Обробка різнорідних великих даних є задачею, яка в сучасності є дуже актуальною, і зустрічається у великій кількості задач, в тому числі й кібербезпеки |
| Чому можна навчитися | В межах дисципліни розглядаються такі питання, як основні принципи аналізу великих гетерогенних даних, джерела гетерогенних даних та принципи їх спільного використання, обробки та аналізу. |
| Як можна користуватися набутими знаннями та вміннями | В результаті вивчення навчальної дисципліни студенти зможуть застосувати методи глибокого навчання для обробки гетерогенних даних; будуть володіти практичними навичками використання інструментів глибокого навчання для розв’язання задач на основі гетерогенних даних великого об’єму. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1wJBJR9oc1U-QbxmPfyER50cyBvoqSjPu?usp=sharing |
| Вид семестрового контролю | екзамен |

# 4. МЕТОДИ ГЛИБОКОГО НАВЧАННЯ НА РІЗНОРІДНИХ ДАНИХ
(проф. Куссуль Н.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичного моделювання та аналізу даних |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для вивчення дисципліни студент має володіти методами лінійної алгебри, теорії ймовірностей і математичної статистики, теорії оптимізації, машинного навчання та аналізу даних, бути знайомим з основами програмування, бажано на Python, а також з класичними алгоритмами та структурами даних. |
| Що буде вивчатися | Дисципліна "Методи глибокого навчання на різнорідних даних" присвячена вивченню методів та технологій машинного навчання з урахуванням сучасних тенденцій розвитку цієї галузі в епоху цифровізації з використанням великих об'ємів гетерогенних даних. |
| 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 | В результаті вивчення навчальної дисципліни студенти зможуть застосувати методи глибокого навчання для обробки гетерогенних даних; будуть володіти практичними навичками використання інструментів глибокого навчання для розв'язання задач на основі гетерогенних даних великого об'єму. |
| Як можна користуватися набутими знаннями та вміннями | Набуті знання можна використовувати в професійній сфері, для наукової роботи та в повсякденному житті. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1wP5lu4ki4foVpaAzugYSgJa6x_Eqobc1?usp=sharing<br>Платформа "Сікорський": курс «Методи глибокого навчання на різнорідних даних» https://do.ipo.kpi.ua/course/view.php?id=1713 |
| Вид семестрового контролю | екзамен |

# 5. ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ТА ЕКСПЛУАТАЦІЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

(доц. Барановський О.М.)

| | |
|---|---|
| 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 | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для успішного оволодіння матеріалом потрібно мати знання та навички із захисту інформації в інформаційно — комунікаційних системах та розуміння принципів захисту Web-ресурсів. |
| Що буде вивчатися | Метою навчальної дисципліни "Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем" є отримання знань та навичок про архітектуру, налаштування та супровід технологій захисту сучасних інформаційно-комунікаційних систем.". |
| Чому це цікаво/треба вивчати | Адміністрування та експлуатація захищених систем є складовою практично будь-яких задач за фахом. |
| Чому можна навчитися | В процесі вивчення дисципліни студент засвоїть 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 | Набуті знання та вміння можна використовувати в професійній діяльності за фахом, а також як допоміжний інструмент при вирішенні інноваційних задач |
| Інформаційне забезпечення | Посилання на силабус: |

| | |
|---|---|
| дисципліни | https://drive.google.com/drive/folders/1RqQfq0p3176IO-5G0wO6DR6JRukbAySN?usp=sharing |
| Вид семестрового контролю | екзамен |

# 6. ТЕОРІЯ ТА МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В КІБЕРБЕЗПЕЦІ

(доц. Стьопочкіна І.В.)

| | |
|---|---|
| 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 | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Загальні знання з інформаційних технологій |
| Що буде вивчатися | Теоретичні основи та практичні техніки атак соціальної інженерії в кібербезпеці, методи захисту від атак соціальної інженерії, відповідне програмне забезпечення. |
| 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 | Технікам соціальної інженерії (для задач offensive security, тестування на проникнення), опанувати засоби та методи протидії. |
| Як можна користуватися набутими знаннями та вміннями | Набуті знання можна використовувати в професійній сфері, для наукової роботи та в повсякденному житті. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1ZbkH_IgEruedfNnJUAC6K7Lz6KI6hAG5?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 |

# 7. РЕФЛЕКСИВНИЙ АНАЛІЗ ПОВЕДІНКИ ВИБОРУ

(доцент Смирнов С.А.)

| | |
|---|---|
| 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 | 5 кредитів ЄКТС |
| 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 (ППР), пов’язані із рефлексивною структурою та станом свідомості людини, що приймає рішення. |
| 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/12lAPX_EZAUGP8c_88Hc2y8bI7AKgRHi-?usp=sharing<br>Посилання на дистанційний ресурс:<br>Платформа “Сікорський”, курс “Рефлексивний аналіз поведінки вибору” https://classroom.google.com/u/1/c/ODIyNTE2ODIzNjZa |
| Вид семестрового контролю | екзамен |

# 8. ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА РОЗПОДІЛЕНІ СИСТЕМИ

(проф. Кудін А.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичних методів захисту інформації |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Знання основ криптографії, зокрема симетричної криптографії та асиметричних 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 | Технологія блокчейн використовується при розв'язанні ряду задач кібербезпеки, які висувають підвищені вимоги щодо надійності та безпеки обміну та зберігання 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 | Набуті знання та уміння можна використовувати при роботі над магістерською, зокрема в задачах захисту персональної інформації (даних та особистого листування), елементів безпеки інтернету речей, захищеного розподіленого документообігу, упередження DDoS-атак та ін. |

| | |
|---|---|
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1VHtSFZcmv3dXa7CAbbgeKG4fFjpHWctY?usp=sharing |
| Вид семестрового контролю | екзамен |

## 9. МОДЕЛІ ТА МЕТОДИ КРИПТОАНАЛІЗУ БЛОКОВИХ ШИФРІВ
(доц. С.В. Яковлєв)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичних методів захисту інформації |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 5 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Базові знання 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>У дисципліні будуть детально розглянуті такі теми:<br>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) модифікації 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) модифікації 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 його 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 їх криптоаналіз. |
| Чому можна навчитися | Студенти отримують знання моделей та методів криптоаналізу блокових шифрів, параметрів стійкості до криптоаналітичних атак та їх 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.<br>Отримані навички та засвоєнні знання можуть використовуватись для проведення наукових та прикладних досліджень у галузі симетричної криптографії, а також для розв'язання прикладних задач у галузі криптографічного захисту інформації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1uUogeDExAda2Wsvs7BJo7K0gtIEjzmBY?usp=sharing |
| Вид семестрового контролю | екзамен |

# ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

## (ЗАЛІКОВІ ДИСЦИПЛІНИ)

## 10. WEB - АНАЛІТИКА

(доц. Ткач В.М.)

| | |
|---|---|
| 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 |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Знання програмування, в тому числі розуміння парадигми об'єктно орієнтованого програмування, та основ 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 | 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. |
| Чому можна навчитися | Вам будуть зрозумілі принципи аналітики даних в |

| | |
|---|---|
| | інтернет, методи визначення аномалій |
| Як можна користуватися набутими знаннями та вміннями | В професійній діяльності та при роботі над магістерською дисертацією |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1iiKKr0iYzB9b6bCwPdJ6aF3T1Gx1u4MK?usp=sharing |
| Вид семестрового контролю | залік |

# 11. ПРОЕКТУВАННЯ РОЗПОДІЛЕНИХ СИСТЕМ

(доцент Родіонов А.М.)

| | |
|---|---|
| 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 |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Знання архітектури та принципів розробки ПЗ, бази даних, мережева взаємодія та протоколи прикладного рівня. Знання будь-якої мови програмування та створення за її допомогою Web-застосувань |
| Що буде вивчатися | Навчальна дисципліна «Проектування розподілених систем» присвячена теоретичним та практичним аспектам створення масштабованих, високонавантажених та високодоступних розподілених систем, а також програмного забезпечення на їх основі.<br>У курсі розглядається базова теорія пов'язана з розподіленими системами і велика частина курсу присвячена мікросервісній архітектурі та шаблонам мікросерівів.<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 | Розподілені системи зараз використовуються у великій кількості компаній, і робота з ними є необхідною вимогою з боку багатьох роботодавців. |
| Чому можна навчитися | Основні теми курсу:<br>– Масштабованість, продуктивність, доступність сучасних застосувань<br>– 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 | При написанні магістерської дисертації та в майбутній професійній діяльності |
| Інформаційне забезпечення дисципліни | Посилання на силабус:<br>https://drive.google.com/drive/folders/1MtHk-5wT6gBYeGCNB1it4LEvMLYyunHR?usp=sharing |
| Вид семестрового контролю | залік |

# 12. РІШЕННЯ В УМОВАХ НЕВИЗНАЧЕНОСТІ ТА РИЗИКУ

(доцент Смирнов С.А.)

| | |
|---|---|
| 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 |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для успішного засвоєння курсу потрібні попередні знання з наступних дисциплін: математичний аналіз, алгебра і геометрія, дискретний аналіз, математичне моделювання. |
| Що буде вивчатися | Метою курсу є вивчення теоретичних основ та практичних методів прийняття рішень в умовах невизначеностей різної природи: множинної, ймовірнісної, 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 проблемної ситуації до результату |
| Як можна користуватися набутими знаннями та вміннями | Відповідні знання знадобляться при розв'язанні задач безпеки, пов'язаних із визначенням ризиків, в умовах дії людського фактору чи інших елементів невизначеності. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/10VqxIQLvYPQJQlYI6RnpHWrDKW7qFsOK?usp=sharing<br>Посилання на дистанційний ресурс:<br>Платформа "Сікорський", курс "Рішення в умовах невизначеності та ризику "<br>https://classroom.google.com/u/1/c/OTk3MTgyNzQzNDNa?hl=uk |
| Вид семестрового контролю | залік |

# 13 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ

(проф. Шелестов А.Ю.)

| | |
|---|---|
| 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 |
| 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 | Дані великого обсягу наразі аналізуються та обробляються великою кількістю систем. Виділяються хмари, озера даних та ін. |
| Чому можна навчитися | Володінню методами та засобами аналізу великих гетерогенних даних |
| Як можна користуватися набутими знаннями та вміннями | Дисципліна "Інформаційні технології аналізу великих гетерогенних даних" присвячена вивченню сучасних засобів аналізу гетерогенних даних та основних інформаційних технологій для роботи з даними великого об’єму з різних джерел.<br>В межах даної навчальної дисципліни розглядаються сучасні інформаційні технології та програмне забезпечення для обробки гетерогенних даних, підходи до обміну та представлення гетерогенної інформації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1gRhpuaXNnVU3VodHFkHpXOTIPUCxMYNx?usp=sharing |
| Вид семестрового контролю | залік |

# 14. ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

(доцент Яковлев С.В.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичних методів захисту інформації |
| Рівень вищої освіти | 2 |
| Курс, семестр | 1 курс, 2 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 4 кредити ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Знання основ криптографії |
| Що буде вивчатися | Навчальна дисципліна «Інфраструктури відкритих ключів» знайомить студентів з принципами, методами та механізмами організації систем керування ключами та захищеного документообігу. |
| Чому це цікаво/треба вивчати | Основною метою дисципліни є формування у студентів знань основних принципів роботи центрів сертифікації ключів, організації життєвого циклу ключів, форматів основних структур даних, які використовуються у механізмах захисту систем захищеного документообігу |
| Чому можна навчитися | Основні теми, які розглядаються у курсі:<br>– електронні довірчі послуги, класифікація електронних підписів та їх функціональність; механізми eIDAS;<br>– життєвий цикл криптографічних ключів, організація керування життєвим циклом ключів, різні варіанти будови інфраструктур відкритих ключів, Центри сертифікації ключів;<br>– мова ASN.1, стандарти кодування BER, CER, DER;<br>– формат сертифікатів відкритих ключів X.509v3;<br>– перевірка статусу сертифікатів, атрибутні сертифікати, списки відкликаних сертифікатів, протокол OCSP;<br>– протоколи керування сертифікатами (PKCS10, CMC, CMP);<br>– формати криптографічних повідомлень (CMS), підписані повідомлення, часові штемпелі; розширені формати підписаних повідомлень (CAdES);<br>– - формати захищених повідомлень |
| Як можна користуватися | Знання основних принципів роботи центрів |

| | |
|---|---|
| набутими знаннями та вміннями | сертифікації ключів, організації життєвого циклу ключів, форматів основних структур даних, дозволяють ввільно почуватися у роботі з механізмами захисту систем захищеного документообігу |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1rkBBOVirSi3zT4j-fL7zy2nb1LAVuY-z?usp=sharing<br><br>Посилання на дистанційний ресурс: Платформа “Сікорський”, курс “Інфраструктури відкритих ключів” https://classroom.google.com/u/1/c/NTI3MTM0MDcxNjc5 |
| Вид семестрового контролю | залік |

## 15. Проактивний захист персональних даних 1
**(доцент, к.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 |
| 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 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. |
| Як можна користуватися набутими знаннями та вміннями | Підвищення точності імітаційного моделювання фізичних процесів та явищ. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1HmIOohA1UNgvZKGaeAPm8PGajj2utadj?usp=sharing |
| Вид семестрового контролю | залік |

## 16. Проактивний захист персональних даних 2

**(доцент, к.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 |
| 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 «Проактивний захист персональних даних 2» є поглиблення у студентів компетентностей з синтезу елементів систем обробки інформації з врахуванням заданих вимог щодо їх взаємодії з іншими елементами та системами. Предметом дисципліни є методи синтезу систем. |
| Чому це цікаво/треба вивчати | Поглиблення розуміння принципів, методів та засобів імітаційного моделювання систем обробки сигналів. Розуміння методів синтезу даних систем за наявними вимогами/параметрами. |
| Чому можна навчитися | – Знання методів декомпозиції та порівняльного аналізу складних систем;<br>– Знання основ конструювання та проектування елементів систем обробки (захисту) інформації;<br>– Знання методів проведення імітаційного моделювання елементів та систем обробки даних;<br>– Вміння побудови імітаційної моделі та синтезу елементів систем обробки (захисту) даних. |

| | |
|---|---|
| Як можна користуватися набутими знаннями та вміннями | Підвищення якості моделювання систем обробки сигналів, синтезу даних систем за наявними параметрами/вимогами. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/10bUR7yiDLnYyhn-jc31Qnje_QY7zgez9?usp=sharing |
| Вид семестрового контролю | залік |

# ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ДРУГОГО КУРСУ НАВЧАННЯ

## (ЗАЛІКОВІ ДИСЦИПЛІНИ)

# 17. БЕЗПЕКА КІБЕРФІЗИЧНИХ СИСТЕМ

(доцент Смирнов С.А.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Курс, семестр | 2 курс, 3 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 4 кредитів ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Для розуміння змісту курсу студентам достатньо мати базові знання з наступних навчальних дисциплін: математичний аналіз, лінійна алгебра, загальна фізика, математичне моделювання. |
| Що буде вивчатися | Навчальна дисципліна орієнтована на оволодіння сучасними кібернетичними та фізичними принципами побудови, функціонування та убезпечення широкого спектру кіберфізичних систем. |
| Чому це цікаво/треба вивчати | Сучасний стан та перспективи розвитку кіберпростору людства багато в чому визначаються т. зв. вбудованими системами, які складають технічну базу Інтернету речей і, таким чином, забезпечують подальше його поширення та проникнення у всі сфери практичної діяльності. Кіберфізичні системи, в свою чергу, є науково-технологічною базою вбудованих систем, яка підтримує імплементацію керуючих та інформаційних процесів у реальні фізичні системи але породжує нові вразливості та загрози. |
| Чому можна навчитися | *знання*: основних принципів організації інформаційних процесів, зв'язку між сигнально-інформаційною та матеріально-енергетичною складовою реальних процесів та явищ; зв'язку між інформацією, прийняттям рішень та їх реалізацією (управлінням); класифікації загроз для систем управління та методів їх аналізу, виявлення та попередження; видів синхронізації, управління синхронізацією та управління хаосом;<br>*уміння*: вільно володіти і оперувати основними поняттями систем управління у фізичному контексті; вміти визначати цілі управління та засоби їх досягнення, характеристики систем управління |

| | |
|---|---|
| | (стійкість, вразливість, керованість, спостережуваність); будувати алгоритми управління на основі градієнтних методів та методу швидкісного градієнту; перевіряти алгоритми керування на вразливості та небезпеки. |
| Як можна користуватися набутими знаннями та вміннями | Курс дозволяє вільно орієнтуватися на якісному і кількісному рівні в основних фізичних принципах, умовах, можливостях, обмеженнях та загрозах, пов'язаних з обробкою та використанням інформації в кіберфізичних системах; виробити навички практичного використання засвоєних знань, методів і підходів у подальшому навчанні та професійній діяльності. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1CVEEybuGa9n_LD1bACSEGEwBxxTH-OmA?usp=sharing<br><br>Посилання на дистанційний ресурс:<br>Платформа "Сікорський", курс "Безпека кіберфізичних систем" https://classroom.google.com/u/1/c/NTI3MTM0MDcxNjc5 |
| Вид семестрового контролю | залік |

# 18. МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

(Проф. Кудін А.М.)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | Математичних методів захисту інформації |
| Рівень вищої освіти | 2 |
| Курс, семестр | 2 курс, 3 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 4 кредити ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Знання основ криптографії |
| Що буде вивчатися | Метою вивчення дисципліни є ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем.<br>Завданням дисципліни є засвоєння студентами вміння адекватно оцінювати стійкість реальних криптосистем, основних алгоритмів їх реалізації, а також встановлення взаємозв‘язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах. |
| Чому це цікаво/треба вивчати | Перехід людства до інформаційного суспільства супроводжується революційними змінами в усіх сферах громадської діяльності, а насамперед – в технології захисту інформаційних ресурсів. Ці зміни поширюються і на всі науки, що досліджують проблеми захисту інформації від навмисних та ненавмисних загроз, в тому числі – криптології. Так в останні роки з’явились численні роботи (зокрема Голдрейха, Гольдвассер та інших), в яких досліджується основи криптології, формулюються специфічні саме для криптології методи досліджень – тобто проходить процес ставлення криптології як самостійної науки, а не тільки як розділу прикладної математики. Іншою рисою останнього часу є створення поняття «відкритої криптографії» і поширення криптографічних методів для захисту інформації в недержавних і «відкритих» автоматизованих системах.<br>Ці фактори призводять до актуалізації проблеми адекватної реалізації базових криптографічних |

| | |
|---|---|
| | примітивів та протоколів, адекватності створених теоретичних моделей криптології реальним ситуаціям, що виникають при їх застосуванні, вміння практичного застосування методів криптології. |
| Чому можна навчитися | Метою вивчення дисципліни є ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем.<br>Завданням дисципліни є засвоєння студентами вміння адекватно оцінювати стійкість реальних криптосистем, основних алгоритмів їх реалізації, а також встановлення взаємозв‘язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах. |
| Як можна користуватися набутими знаннями та вміннями | Курс може бути використаний при створенні та експлуатації систем захисту інформації, а також при проведенні сертифікації та експертизи засобів захисту інформації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1WSYvmD97XeUe9rrc_ptiK7gqaySL6kWZ?usp=sharing |
| Вид семестрового контролю | залік |

# 19. МОДЕЛІ ЦІННОСТІ ІНФОРМАЦІЇ ТА ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОГО ЗАХИСТУ

(Проф. М.М. Савчук )

| | |
|---|---|
| Кафедра, яка забезпечує викладання | ММЗІ |
| Рівень вищої освіти | 2 |
| Курс, семестр | 2 курс, 3 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 4 кредити ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Базові знання з алгебри, дискретної математики, комбінаторики, теорії ймовірностей та математичної статистики, а також розуміння основних концепцій криптології. |
| Що буде вивчатися | Теоретичні поняття інформації, цінності інформації, різних способів означення та вимірювання цінності інформації, поняття дезінформації з точки зору цінності інформації, а також аспекти практичного застосування цих питань до проблем оцінювання стійкості криптографічних примітивів та розширення поняття цілком таємних систем за Шенноном. |
| Чому це цікаво/треба вивчати | Сучасні дослідження в галузі обробки, передачі, захисту інформації та криптологічних досліджень суттєво враховують цінність інформації, що передається та захищається. |
| Чому можна навчитися | Застосовувати моделі цінності інформації для побудови і дослідження систем передачі та захисту інформації з урахуванням цінності інформації. вибирати і використовувати різні поняття стійкості для оцінки ефективності інформаційних систем і надійності захисту інформації. |
| Як можна користуватися набутими знаннями та вміннями | Отримані навички та засвоєнні знання можуть використовуватись для проведення наукових та прикладних досліджень при побудові та оптимізації |

| | |
|---|---|
| | інформаційних систем, а також для розв'язання прикладних задач у галузі безпеки інформації та криптографічного захисту інформації. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1JaG4gdIVkMnhHOE0FePbrp8wegiVyI26?usp=sharing |
| Вид семестрового контролю | залік |

# 20. МОДЕЛЮВАННЯ СКЛАДНИХ СИСТЕМ

(ст. викладач, к.ф.-м.н. О. В. Рибак)

| | |
|---|---|
| Кафедра, яка забезпечує викладання | інформаційної безпеки |
| Рівень вищої освіти | 2 |
| Курс, семестр | 2 курс, 3 семестр |
| Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи | 4 кредити ЄКТС |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Основними інструментами дисципліни «Моделювання складних систем» є теорія ймовірностей і математична статистика, теорія графів, теорія клітинних автоматів, агентне моделювання. |
| Що буде вивчатися | Курс «Моделювання складних систем» дає змогу оволодіти умінням застосовувати значну кількість математичних методів і адаптивних інструментів моделювання для дослідження взаємодії технічних і соціальних систем. Теоретичні матеріали курсу дають студенту знання про: 1) лінійні моделі та методи їх регуляризації; 2) методи побудови нелінійних моделей; 3) моделі змішаного типу (SWM метод); 4) байєсівські моделі складних структурних відношень; 5) ансамблі моделей (випадковий ліс, бустінг, бегінг). |
| Чому це цікаво/треба вивчати | Дисципліна «Моделювання складних систем» розглядається як міждисциплінарна область знань на границі інформатики та кібербезпеки, Вона фокусується на системах забезпечення безпеки, що є складними системами з великою кількістю взаємодіючих компонентів. |
| Чому можна навчитися | Внаслідок виконання практичних завдань студент набуває такі уміння: 1) застосовувати багатомодельний підхід до розуміння складних явищ і процесів; 2) оцінювати параметри моделей; 3) відбирати підмножини змінних; 4) знижувати розмірність ознакового простору; 5) отримувати додаткову інформацію про параметри моделі за допомогою перехресної перевірки та бутстреп методу; 6) оцінювати ефективність розробленої моделі. |
| Як можна користуватися набутими знаннями та вміннями | В роботі з складними системами допоможуть знання та навички з декомпозиції та спрощення, |

| | |
|---|---|
| | агрегування систем, вміння розділяти та поєднувати, досліджувати окремі компоненти. Знання, набуті студентами під час вивчення курсу «Моделювання складних систем», дозволять ліпше розуміти, пояснювати, розробляти, прогнозувати і досліджувати складні явища та процеси, що відбуваються у реальних системах. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1wqIWYN4guBZIwYRFvKifP5UO0wZMu6Zx?usp=sharing |
| Вид семестрового контролю | залік |

## 21. ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(доцент, к.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 |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | вчання на програмі дуальної освіти з Samsung R&D раїна |
| Що буде вивчатися | Метою дисципліни є формування компетентностей з застосування методів машинного навчання в задачах захисту конфіденційних даних, що обробляються на мобільних пристроях. Досліджуються задачі щодо розробки й оцінки ефективності автоматизованих систем виявлення шкідливого програмного забезпечення (ШПЗ) в умовах обмеженості апріорних даних щодо його особливостей. |
| Чому це цікаво/треба вивчати | Поглиблення розуміння сучасних підходів до ідентифікації систем обробки даних за наявними (частковими) даними. Розуміння методів непрямого визначення параметрів системи обробки даних. |
| Чому можна навчитися | – знання основ математичної статистики та теорії ймовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності, знання основ роботи зі штучними нейронними мережами<br>– навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, Keras/TensorFlow, MATLAB Simulink)<br>– знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS. |
| Як можна користуватися набутими знаннями та вміннями | За результатами вивчення дисципліни студенти отримають знання щодо розробки методів поведінкового аналізу на основі штучних нейронних мереж, а також навики виявлення ШПЗ в умовах обмеженості апріорних даних щодо його |

| | |
|---|---|
| | особливостей. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1Ihu6JKrgQgGmjZvhmtCuvvbLycZ6cuyq?usp=sharing<br><br>- Murphy Kevin P. Machine Learning: A Probabilistic Perspective. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2012. – 1104 p. – ISBN 978-0262018029.<br>- Bishop Christopher M. Pattern Recognition and Machine Learning. – Information Science and Statistics series. – Springer, 2011. – 738 p. – ISBN 978-0387310732. |
| Вид семестрового контролю | залік |

# 22. ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

(доцент, к.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 |
| Мова викладання | українська |
| Вимоги для початку вивчення дисципліни | Навчання на програмі дуальної освіти з Samsung R&D Україна |
| Що буде вивчатися | Метою дисципліни є формування компетентностей з застосування методів машинного навчання розробки автоматизованих систем обробки персональних даних, зокрема поведінкових систем автентифікації. |
| Чому це цікаво/треба вивчати | Досліджуються задачі щодо оцінки ефективності сучасних систем поведінкової автентифікації користувачів на мобільних пристроях. |
| Чому можна навчитися | – Знання основ математичної статистики та теорії ймовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності, знання основ роботи зі штучними нейронними мережами;<br>– навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, Keras/TensorFlow, MATLAB Simulink, MathCAD);<br>– знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS. |
| Як можна користуватися набутими знаннями та вміннями | За результатами вивчення дисципліни студенти отримають знання та навички щодо розробки та оцінки ефективності методів поведінкової автентифікації користувачів на мобільних пристроях з використанням штучних нейронних мереж. |
| Інформаційне забезпечення дисципліни | Посилання на силабус: https://drive.google.com/drive/folders/1iTQyc9eVKU8c1jfqEjXyv937C2paMPng?usp=sharing |

| | |
|---|---|
| | - Murphy Kevin P. Machine Learning: A Probabilistic Perspective. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2012. – 1104 p. – ISBN 978-0262018029.<br>- Bishop Christopher M. Pattern Recognition and Machine Learning. – Information Science and Statistics series. – Springer, 2011. – 738 p. – ISBN 978-0387310732. |
| Вид семестрового контролю | залік |