ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

ФІЗИЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЗАТВЕРДЖЕНО

на засіданні кафедри твердотільної електроніки
та інформаційної безпеки
протокол № 9 від «15» червня 2023 р.

Завідувач кафедри _____ проф. Різак В.М.

Каталог вибіркових навчальних дисциплін кафедри твердотільної електроніки та інформаційної безпеки

освітньої програми “Безпека інформаційних і комунікаційних систем” за спеціальністю 125 Кібербезпека та захист інформації

другого (магістерського) рівня вищої освіти

УЖГОРОД - 2023

ЗМІСТ

Технології створення та застосування систем захисту інформаційно-комунікаційних систем

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни, список джерел для вивчення дисципліни, завдання для самостійної роботи студентів, ресурси Cisco NetAcad.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання:

Метою навчальної дисципліни «Технології створення та застосування систем захисту інформаційно-комунікаційних систем» є формування у студентів компетентностей зі створення та обслуговування сучасних інформаційних систем.

Завданнями даного курсу є оволодіння студентами основними методами і принципами побудови систем безпекового моніторингу та реагування на інциденти, а також вільного використання організаційних, технічних та програмних методів захисту інформації.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

1. Вступ. Куб кібербезпеки.
2. Глобальні центри інформаційної безпеки та керування кібербезпекою.
3. Захист мережі.
4. Захист кінцевих пристроїв.
5. Шифрування та інфраструктура відкритих ключів.
6. Захист кінцевих пристроїв.
7. Аудит мережної активності.
8. Моніторинг безпеки.
9. Аналіз даних по вторгненням.
10. Реагування на інциденти та їх обработка

Оптоволоконні комунікаційні системи

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни, список джерел для вивчення дисципліни, завдання для самостійної роботи студентів.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання:

Метою навчальної дисципліни «Оптоволоконні комунікаційні системи» є формування у студентів чіткого розуміння принципів побудови інформаційно-телекомунікаційних систем з використанням волоконно-оптичних технологій.

Завданнями даного курсу є оволодіння студентами основними методами і принципами побудови оптоволоконних комунікаційних систем на базі сучасних методів, а також знання всіх елементів, необхідних для побудови даних систем.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

1. Вступ. Перспективи розвитку оптоволоконних комунікаційних систем, Оптичний діапазон, властивості, параметри і характеристики.
2. Зона застосування оптоволоконних комунікаційних систем.
3. Елементи оптоволоконних комунікаційних систем.
4. Поняття мультиплексування. Технології мультиплексування.
5. Синхронна цифрова ієрархія SDH.
6. Плезіохронна цифрова ієрархія PDH.
7. Підсилення оптичних сигналів. Регенераційна ділянка.
8. Параметри та характеристики оптичних підсилювачів.
9. Моделі оптичних мереж.
10. Мультисервісне оптичне обладнання XDM.
11. Архітектура обладнання XDM.

Автоматизація обробки даних з обмеженим доступом

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни, список джерел для вивчення дисципліни, завдання для самостійної роботи студентів.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання:

Метою навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом» є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації з обмеженим доступом в умовах опрацювання значних об’ємів даних.

Завданнями даного курсу є оволодіння студентами основними методами і принципами побудови автоматизованих систем обробки інформації з обмеженим доступом, а також вільного використання організаційних, технічних та програмних методів захисту інформації під час обробки великих масивів даних.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

1. Вступ. Інформація з обмеженим доступом (ІзОД) та способи її захисту під час автоматизованої обробки
2. Кіберзахист об’єктів критичної інфраструктури
3. Формування вимог до комплексних систем захист інформації в АС та ІТС
4. Проектування системи автоматизованої обробки інформації з обмеженим доступом
5. Реалізація системи автоматизованої обробки інформації з обмеженим доступом.
6. Функції та можливості програмного засобу захисту інформації «ЛОЗА™-1, версія 4» від несанкціонованого доступу в автоматизованих системах класу «1».
7. Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс "Гриф" версії 5».
8. Особливості захисту інформації в автоматизованих системах класу «2». Комплекс засобів захисту «Гриф-Мережа».
9. Автоматизація обробки інформації з обмеженим доступом засобами мови Python.
10. Автоматизація роботи з файлами та створення баз даних ІзОД

Широкосмугові сигнали в системах ТЗІ

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	«Основи теорії кіл, сигнали та процеси в електроніці», «Бездротові ІКС та їх проектування», «Технології створення та застосування систем захисту ІКС»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Підручники, навчальні посібники, методичні рекомендації, мультимедійний проєктор.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- Розуміння фізичних основ формування сигналів в різних фізичних середовищах передачі сигналів;
- Вміння оцінювати співвідношення сигнал завада в різних умовах формування передачі та отримання сигналу;
- Розуміння принципів побудови систем передачі, формування, отримання широко смугових сигналів;
- Навички оцінки та атестації систем передачі широкосмугового сигналу;
- Вміння моделювати, досліджувати широкосмугові сигнали засобами математичного моделювання

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Динамічні моделі періодичного сигналу. Гармонічні базиси спектру неперервного сигналу. АКФ, ДПФ сигналів. Білий шум. АКФ, ВКФ дискретного сигналу. Спектри сигналів. Гармонічні завади. Видалення гармонічних та імпульсних завад.

Технології стиску інформаційних потоків

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	«Основи теорії кіл, сигнали та процеси в електроніці», «Інформаційні технології», «Комп'ютерна схемотехніка», «Теорія розподілених інформаційних ресурсів, захист баз даних та знань», «Бездротові ІКС та їх проектування», «Технології адміністрування та експлуатація захищених ІКС», «Технології створення та застосування систем захисту ІКС»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Підручники, навчальні посібники, методичні рекомендації, мультимедійний проєктор
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- здатність застосовувати загальні принципи статистичних методів стиснення;
- здатність застосовувати загальні принципи словникових методів стиснення;
- здатність застосовувати методи стиснення статичних зображень;
- здатність аналізувати й застосовувати методи стиснення відео аудіо даних виявлення/вкладання приховуваної інформації за поняттями кібербезпеки;
- здатність застосовувати основні метрики, що характеризують ефективність процедур стиснення-відновлення даних з точки зору кібербезпеки

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Цифрові технології - головні ознаки нової інформаційної цивілізації. Класи технологій стиску інформаційних потоків. Статистичні та словникові методи кодування. Кольорові простори RGB, YCbCr. Методи трансформації зображення: дискретне косинусне та вейвлет перетворення. Алгоритми стиснення даних як методи передачі прихованої інформації. Стандарти стиснення статичних та динамічних (відео) інформаційних потоків. Стиснення аудіо-даних.

Системи захисту мовної інформації на об’єктах інформаційної діяльності

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	“Виявлення та попередження кіберінцидентів”, “Технології створення та застосування комплексів захисту інформації з обмеженим доступом”
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Підручники, навчальні посібники, методичні рекомендації, мультимедійний проєктор.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
- Розробляти, застосовувати, інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки.
- Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі нових результатів досліджень інженерних і фізико- математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
- Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
- Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
- Забезпечувати неперервність бізнес/операційних процесів, виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури контролю та розслідування, а також надавати рекомендації щодо попередження кіберінцидентів в цілому.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Тема 1. Основні джерела витоку інформації
Тема 2. Класифікація джерел витоку мовної інформації
Тема 3. Основи захисту мовної інформацій
Тема 4, Методи протидії витоку мовної інформації
Тема 5. Класифікація методів протидії витоку мовної інформації
Тема 6. Організаційні методи протидії витоку мовної інформації
Тема 7. Фізичні методи протидії витоку мовної інформації
Тема 8, Апаратно прогрмні методи протидії витоку мовної інформації
Тема 9. Комплексні системи захисту мовної інформації
Тема 10. Стандартизація та сертифікація комплексів захисту мовної інформації

Автоматизоване проектування технічних засобів захисту інформації

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни,
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- уявлення про мету, завдання і принципи функціонування технічних систем захисту інформації, про способи і методи захисту інформації від витоку технічними каналами;
- знання принципів проектування, функціонування та супроводу систем технічного захисту інформації;
- розуміння принципів функціонування технічних засобів захисту інформації;
- розуміння фізичних та логічних основ проектування технічних засобів захисту інформації;
- використання методів методи забезпечення конфіденційності та відновлення цілістності інформації;
- вміння застосовувати набуті знання та навики для проектування технічних систем захисту інформації;
- уміння забезпечувати ефективне функціонування технічних засобів захисту інформації;
- контролювати ефективність технічних засобів захисту інформації при їх практичному використанні.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

1. Технічні канали витоку інформації: основні поняття, класифікація.
2. Способи несанкціонованого зняття інформації з технічних каналів витоку інформації.
3. Методи та засоби блокування технічних каналів витоку інформації.
4. Технічні засоби захисту інформації (ТЗЗІ), їх класифікація.
5. Критерії вибору ТЗЗІ.
6. Системи автоматизованого проектування для засобів ТЗІ.

Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	«Основи теорії кіл, сигнали та процеси в електроніці», «Інформаційні технології», «Комп'ютерна схемотехніка», «Теорія розподілених інформаційних ресурсів, захист баз даних та знань», «Бездротові ІКС та їх проектування», «Технології адміністрування та експлуатація захищених ІКС», «Технології створення та застосування систем захисту ІКС»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Підручники, навчальні посібники, методичні рекомендації, мультимедійний проєктор.
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- Здійснювати збір, аналіз і систематизацію науково-технічної інформації з питань протидії витоку інформації з обмеженим доступом радіоелектронними каналами
- Застосовувати на практиці засоби радіомоніторингу і методики їх застосування;
- Користуватись здобутими знаннями для вирішення задач аналізу оперативної обстановки в умовах необхідності використання методів і засобів радіопротидії
- Розглядати пропозиції щодо вдосконалення засобів радіомоніторингу і радіопротидії, які спрямовані на поліпшення якості захисту інформації, давати висновки про доцільність використання засобів радіомоніторингу на об'єктах інформаційної діяльності
- Проводити експериментальні дослідження у сфері радіомоніторингу і радіопротидії

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Тема 1. Основні завдання та умови проведення радіомоніторингу
Тема 2. Радіоканал, як канал витоку інформації
Тема 3. Радіомоніторинг у структурі загальних методів захисту акустичної інформації.
Тема 4, Засоби радіомоніторингу і методики їх застосування
Тема 5. Індикаторні засоби радіомоніторингу
Тема 6. Види завад та засоби їхнього створення
Тема 7. Оцінка ефективності засобів радіозаглушення

Кібергігієна та кібербулінг

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни, список джерел для вивчення дисципліни, завдання для самостійної роботи студентів
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- *Метою навчальної дисципліни* «Кібергігієна та кібербулінг» є набуття знань, умінь та навичок у студентів, удосконалення компетентності щодо основ інформаційної безпеки, особливостей та перспектив забезпечення інформаційної безпеки особи та суспільства, методів протистояння соціальній інженерії, захисту персональних даних, а також протидії кібербулінгу.
- *Завданням даного курсу* є оволодіння студентами практичних та теоретичних навичок у сфері кібергігієни та протидії кібербулінгу, а також формування у них компетентностей необхідних для ефективного застосування кібергігієни в різних сферах діяльності.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Загальні поняття та важливість кібергігієни. Безпека мобільних пристроїв: загальні засади, дозволи застосунків, шкідливе ПЗ. Безпечна робота з онлайн-сервісами та застосунками: політика конфіденційності, безпека паролів, двофакторна автентифікація, контроль над власними даними, використання публічних мереж Wi-Fi, використання VPN. Соціальні мережі та їх вплив, розповсюдження приватних даних. Безпечна робота з ПК: огляд шкідливого ПЗ, використання антивірусного ПЗ, безпечне використання фізичних накопичувачів. Соціальна інженерія, методи та захист від її використання. Фейки та дезінформація, вплив, види, розпізнавання та протидія. Кібербулінг, його ознаки та різновиди. Боротьба з кібербулінгом.

Cisco Certified CyberOps Associate

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська, англійська
Передумови для вивчення дисципліни	Курси мережевої академії Cisco “Introduction to Cybersecurity”, “Introduction to IoT”, “Cybersecurity Essentials”
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Cisco Networking Academy, CyberOps Associate (English - 1.02)
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

CyberOps Associate v1.0 covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC). Upon completion of the CyberOps Associate v1.0 course, students will be able to perform the following tasks:

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Explain how to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

1. The Danger
2. Fighters in the War Against Cybercrime
3. The Windows Operating System
4. Linux Overview
5. Network Protocols
6. Ethernet and Internet Protocol (IP)
7. Principles of Network Security

8. Address Resolution Protocol
9. The Transport Layer
10. Network Services
11. Network Communication Devices
12. Network Security Infrastructure
13. Attackers and Their Tools
14. Common Threats and Attacks
15. Observing Network Operation
16. Attacking the Foundation
17. Attacking What We Do
18. Understanding Defense
19. Access Control
20. Threat Intelligence
21. Public Key Cryptography
22. Endpoint Protection
23. Endpoint Vulnerability Assessment
24. Technologies and Protocols
25. Network Security Data
26. Evaluating Alerts
27. Working with Network Security Data
28. Digital Forensics and Incident Analysis and Response

Ліцензування, атестація та сертифікація у сфері безпеки об’єктів інформаційної діяльності

Рівень вищої освіти	Другий (магістерський)
Курс (рік) навчання	1
Семестр	1, 2
Обсяг дисципліни у кредитах	4
Мова викладання	Українська
Передумови для вивчення дисципліни	Базується на загальних компетентностях випускників ОС «Бакалавр»
Кафедра, яка забезпечує викладання дисципліни	Твердотільної електроніки та інформаційної безпеки
Інформаційне забезпечення	Електронний конспект лекцій, робоча програма дисципліни, методичні матеріали з навчальної дисципліни,
Форма проведення занять	Лекції, лабораторні роботи
Форма семестрового контролю	Залік

Ключові результати навчання(знання, уміння та інші компетентності):

- уявлення про мету і завдання процедури ліцензування господарської діяльності в галузі технічного і криптографічного захисту інформації, призначення та особливості проведення атестації комплексів захисту та сертифікації засобів технічного захисту інформації;
- знання переліку та змісту нормативних документів, якими визначаються ліцензування, атестація та сертифікація у сфері безпеки об’єктів інформаційної діяльності;
- знання правил документального супроводу процедури ліцензування господарської діяльності у сфері захисту інформації;
- розуміння принципів регулювання діяльності із забезпечення захисту інформації;
- знання основ проектування, уведення в експлуатацію та супроводу систем технічного та криптографічного захисту інформації;
- уміння застосовувати набуті знання та навики для проведення процедур атестації комплексів захисту інформації та сертифікації технічних засобів захисту інформації;
- уміння здійснювати проектування, створення та впровадження систем та засобів захисту інформації у відповідності до вимог нормативних документів;
- контролювати ефективність функціонування систем захисту інформації при їх практичному використанні шляхом проведення експертизи та сертифікації.

Короткий зміст дисципліни (що буде вивчатися, перелік тем):

Ліцензійні умови ведення господарської діяльності, пов’язаної із захистом інформації та інформаційних систем. Форми документів. Перелік законодавчих та нормативно-правових актів, що визначають провадження ліцензованої діяльності у галузі КЗІ та ТЗІ. Розробка та впровадження системи технічного захисту інформації на об’єкті інформаційної діяльності. Перелік нормативних документів. Сертифікація технічних та криптографічних засобів захисту інформаційних ресурсів. Атестація комплексу захисту інформації на об’єкті інформаційної діяльності, де циркулює інформація з обмеженим доступом. Експертиза у сфері ТЗІ. Експертний висновок. Сертифікат відповідності.