Силабус навчальної дисципліни

# *Безпека транзакцій у відкритих системах*

***В.А. Золотарьов,***
***доцент. каф. ІМІ, к.т.н., доцент***
***E-mail: vadym.zolotarov@nure.ua***

| Назва поля | Детальний контент, коментарі |
|---|---|
| Назва факультету | Факультет інфокомунікацій |
| Рівень вищої освіти | Другий (магістерський) |
| Код і назва спеціальності | 172 Телекомунікації та радіотехніка |
| Тип і назва освітньої програми | ОПП «Інформаційно-мережна інженерія»» |
| Назва дисципліни | Безпека транзакцій у відкритих системах |
| Кількість ЄКТС кредитів | 4 |
| Структура дисципліни (розподіл за видами та годинами навчання) | 24 год – 12 лекцій,<br>16 год – 4 лабораторних заняття,<br>8 год – 4 консультацій,<br>72 год – самостійна робота,<br>**вид контролю**: залік |
| Графік (терміни) вивчення дисципліни | 1-й рік, I семестр |
| Передумови для навчання за дисципліною | Раніше мають бути вивчені дисципліни за першим (бакалаврським) рівнем освіти спеціальності 172 Телекомунікації та радіотехника |
| Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання | Навчальна дисципліна використовується для формування наступних компетентностей: в процесі практичної діяльності в галузі інфокомунікацій навичками по забезпечуванню інформаційної безпеки мережі; вибору апаратно-технічного, криптографічного та програмного забезпечення для конкретної мережі; вміти виявляти та перекривати технічні канали витоку інформації |
| Якість освітнього процесу | Навчально-методичне та матеріально-технічне ресурсне забезпечення освітньої програми, в рамках якої проводиться вивчення дисципліни, відповідає лицензійним вимогам та акредитаційним умовам провадження освітньої діяльності університету. Здійснюється щорічний моніторінг та перегляд навчальної програми дисципліни у відповідності до вимог та рекомендацій МОН, державної атестації щодо набутих компетентностей випускників, стандартів співпраці з роботодавцями щодо забезпечення конкурентоспроможного рівня підготовки фахівців. Дотримання принципів академічної доброчесності (https://lib.nure.ua/plagiat). Містить публічну інформацію щодо вимог, компетенцій, рівня освіти в рамках дійсної освітньої програми. |

## Опис та зміст дисципліни

Мета вивчення дисципліни - здобування знань, навичок і прийомів роботи з програмними та апаратними засобами захисту інформації, такими як криптографічні пакети, програмно-апаратні комплекси мережного захисту, антивірусне програмне забезпечення та інше; здобування спеціальних знань та практичних навичок у використанні сучасних інформаційних технологій у професійній діяльності.

## Зміст

**Змістовний модуль 1.** Парадигма інформаційної безпеки відкритих систем
Тема 1. Міжнародні критерії оцінювання інформаційної безпеки відкритих систем
Тема 2. Потенційні нападники на відкриті системи, хакерство, комп'ютерна криміналістика
Тема 3. Віддалені атаки на відкриті системи
Тема 4. Класифікація та характеристика методів та засоби отриманняінформації з відкритих систем
**Змістовний модуль 2.** Захист від віддалених атак на відкриті мережі
Тема 1. Захист від віддалених атак, спрямованих на перехоплення даних користувачів та виявлення даних про відкриту мережу
Тема 2. Захист від віддалених атак, спрямованих на виявлення даних про відкриту систему
Тема 3. Захист від віддалених атак, спрямованих на відмову в обслуговуванні
Тема 4. Захист від віддалених атак «Spoofing»
Тема 5. Захист від віддалених атак, спрямованих на отримання доступу до операційного середовища
Тема 6. Захист від віддалених атак типу ін'єкція
**Змістовний модуль 3.** Апаратно-програмні засоби захисту інформації у відкритих системах
Тема 1. Мережні екрани Firewalls та віртуальні приватні мережі VPN
Тема 2. Мережні протоколи із захисту даних
Тема 3. Резервне копіювання даних (backup strategies)
Тема 4. Комп'ютерні віруси та MALWARE, антивірусні програми, паролі

## Результати навчання здобувача вищої освіти

За результатом вивчення дисципліни студенти повинні:

**знати:** основні тенденції розвитку інфокомунікаційних відкритих систем, кіберзагрози інформації; застосування технологій по захисту інформації в інфокомунікаціях від віддалених атак; нормативно-правову базу використання технічних та програмних засобів захисту інформації в інфокомунікаційних

відкритих системах; види захисного програмного забезпечення та їх призначення; криптографічні засоби захисту інформації; можливості використання програмних засобів для обмеження доступу до електронних документів як на локальному ПК так і через інформаційно-комунікаційну мережу, за допомогою стандартних засобів шифрування інформації;

**вміти:** забезпечувати конфіденційність особистої та службової інформації за допомогою отримання теоретичних знань та практичних навиків; користуватися нормативно-правовою базою у галузі інформаційної безпеки; визначати інформацію, що підлягає захисту; впроваджувати і використовувати обрані заходи забезпечення інформаційної безпеки; використовувати свої теоретичні знання та практичні навики для виявляти загроз інформації; аналізувати інформаційні ризики; здійснювати вибір засобів захисту.

**володіти:** в процесі практичної діяльності в галузі інфокомунікацій навичками по забезпечуванню інформаційної безпеки мережі; вибору апаратно-технічного, криптографічного та програмного забезпечення для конкретної мережі; вміти виявляти та перекривати технічні канали витоку інформації.

## Система оцінювання відповідно до кожного завдання для складання заліку/екзамену

Для оцінювання роботи студента протягом семестру підсумкова рейтингова оцінка $O_{сем}$ розраховується як сума оцінок за різні види занять та контрольні заходи

| **Види занять / контрольний захід** | **Оцінка** |
|---|---|
| Лабораторні роботи № 1, 2 | (6…10) x 2 = 12….20 |
| Контрольна робота №1 | (6…10) = 6…10 |
| Контрольна робота №2 | (6…10) = 6…10 |
| **Контрольна точка № 1** | **24…40** |
| Лабораторні роботи № 3, 4 | (6….10)x2 = 12….20 |
| Контрольна робота № 3 | (6…10) = 6…10 |
| Контрольна робота № 4 | (6…10) = 6…10 |
| **Контрольна точка № 2** | **24…40** |
| Індивідуальне домашнє завдання | 12…20 |
| **Разом** | **60…100** |

Як форма підсумкового контролю для дисципліни ЗІТКС використовується залік, під час якого відбувається захист індивідуального домашнього завдання.

### Якісні критерії оцінювання в національній шкалі та ECTS

**Критерії оцінювання роботи студента протягом семестру.**

*Задовільно, D, E (60-74).* Мати мінімум знань і умінь. Відпрацювати та захистити всі лабораторні роботи та ІДЗ.

*Добре, C (75-89).* Знати основні теми дисципліни. Відпрацювати та

захистити всі лабораторні роботи та практичні завдання та ІДЗ.

*Відмінно, A, B (90-100).* Знати всі теми дисципліни. Відпрацювати та захистити всі лабораторні роботи, практичні завдання, пропущені лекції та ІДЗ. Виконати без зауважень всі практичні знання з класичної криптографії. Підготувати реферати по кожному зі змістовних модулів.

## Шкала оцінювання: національна та ECTS

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсового проекту (роботи), практики | для заліку |
| 90 – 100 | **A** | відмінно | зараховано |
| 82-89 | **B** | добре | |
| 74-81 | **C** | | |
| 64-73 | **D** | задовільно | |
| 60-63 | **E** | | |
| 35-59 | **FX** | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного складання |
| 0-34 | **F** | незадовільно з обов'язковим повторним вивченням дисципліни | не зараховано з обов'язковим повторним вивченням дисципліни |

## Методичне забезпечення

### Базова література

1. Золотарьов В. Захист інформації в телекомунікаційних системах // Інформаційні мережі зв'язку. Ч.4 Технології надання інформаційних послуг: навч. Посібник / Безрук В.М., Корольов В.М., Золотарьов В.А., Боцман П.Д., Костромицький А.І., Астраханцев А.А., Капуста С.О. . – Харків:ХНУРЕ,2011. – с.324-391.
2. Климаш М.М., Лунтовський А.О. Інформаційна безпека розподілених систем. Монографія.- Львів: Національний університет «Львівська політехніка», 2014. – 480 с.

### Допоміжна література

1. CUA-14-01A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з некоректним налаштуванням DNS- серверів. – К., ДСТЗІ, 2014. – 12 с.
2. CUA-14-02A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу SNMP. - К., ДСТЗІ, 2014. – 10 с.
3. CUA-14-03A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу SSDP. - К., ДСТЗІ, 2014. – 10 с.
4. CUA-14-04A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу NetBIOS - К., ДСТЗІ, 2014. – 10 с.

5. CUA-14-05A Рекомендації CERT-UA для усунення вразливостей, пов’язаних з некоректним налаштуванням NTP- серверів/ - К., ДСТЗІ, 2014. – 8 с.
6. CUA-15-01M Опис шкідливого програмного забезпечення Regin. - К., ДСТЗІ, 2015. – 13 с.
7. CUA-15-04R Рекомендації CERT-UA з протидії загрозі інсайдера. - К., ДСТЗІ, 2015. – 13 с.
8. CUA-15-05R БЕЗПЕКА ПОШТОВОГО СЕРВІСУ. - К., ДСТЗІ, 2015. – 9 с.

**Методичні вказівки та література до різних видів занять**

1. Методичні вказівки до лабораторних робіт з дисципліни «Захист інформації в телекомунікаційних системах» для студентів напряму «Телекомунікації» спеціальності 8.092402 – Інформаційні мережі зв’язку. Упоряд.: В.А.Золотарьов, А.А.Астраханцев, О.В.Федоров,. – Харків, ХНУРЕ, 2008. – 108 с.
2. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. -Дніпропетровськ.: Національний гірничий університет, 2013. - 318 с.
3. Поляков Н.Л., Тищенко А.В. Математические основы криптографии. Задачи и решения. – М.: Финансовый университет, 2015. – 25 с.
4. Правовий захист інформації. Навчальний посібник. / Н.І.Логінова, Р.Р.Дорожбур – Одеса, Фенікс, 2015 – 264 с.

**Інформаційне забезпечення**

1. Оригінальне програмне забезпечення