# СИЛАБУС ДИСЦИПЛІНИ «БЕЗПЕКА БЕЗПРОВІДНИХ, МОБІЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ»

**Ступінь вищої освіти – Бакалавр**
**Спеціальність 125 – КІБЕРБЕЗПЕКА**
**Освітня програма «Кібербезпека»**
**Рік навчання 2, семестр 4**
**Форма навчання** денна
**Кількість кредитів ЄКТС 4**
**Мова викладання** українська

| | |
|---|---|
| **Лектор курсу** | **Лахно Валерій Анатолійович, д.т.н., професор (портфоліо)** |
| |  |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail lva964@nubip.edu.ua** |
| **Сторінка курсу в eLearn** | **ЕНК (4 семестр)** |

## ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає формування теоретичних знань і придбання практичних умінь і навичок з питань використання технологій захищених розподілених обчислень, віртуалізації серверних систем, проектування захищених корпоративних обчислювальних систем із застосуванням безпровідних, мобільних і хмарних обчислень.

**Навчальна дисципліна забезпечує формування ряду фахових компетентностей**:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

**Спеціальні (фахові, предметні) компетентності (СК):**

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

**У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме**

РН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

РН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

РН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

РН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

**Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання**.

## СТРУКТУРА КУРСУ

| Тема | **Години** (лекції/ Лабораторні,) | **Результати навчання** | **Завдання** | **Оцінювання** |
|---|---|---|---|---|
| **4 семестр** | | | | |
| **Модуль 1. Концепція динамічної маршрутизації.** | | | | |
| Тема 1. Центр моніторингу та керування безпекою. | **2/2** | Введення в основи моніторингу та спеціалізованих структур керування безпекою. | Теоретичне опитування. | **5** |
| Тема 2. Бездротові технології та їх протоколи. | **2/2** | Дослідження бездротових технологій та їх протоколів. | Здача лабораторної роботи. | **10** |

| | | | | |
|---|---|---|---|---|
| Теми 3. Загрози та вразливості мобільних додатків, мобільних пристроїв. | **4/4** | Аналіз та дослідження загроз та вразливостей мобільних додатків та мобільних пристроїв. | Здача лабораторної роботи.<br><br>Опитування | **10**<br><br>**5** |
| Тема 4. Мережеві протоколи та служби. | **2/2** | Вивчення основних мережевих протоколів та принципів їх роботи. | Здача лабораторної роботи. | **10** |
| Тема 5. Мережева інфраструктура для бездротових мереж. | **2/2** | Основи побудови бездротової мережі на основі різних пристроїв та технологій. | Здача лабораторної роботи. | **10** |
| Тема 6. Загрози та вразливості Wi-Fi-мереж та їх захист. | **2/2** | Дослідження загроз та вразливостей WiFi-мереж. | Здача лабораторної роботи. | **10** |
| Тема 7. Хмарні технології та основи побудови інфраструктури. | **2/2** | Дослідження побудови хмарної інфраструктури. | Здача лабораторної роботи. | **10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **30** |
| **Модуль 2. Забезпечення безпровідних, мобільних та хмарних технологій.** | | | | |
| Тема 1. Принципи забезпечення безпеки у бездротових мережах. Моніторинг безпеки бездротових мереж. | **4/4** | Дослідження документування подій у мережі, автоматизація записів. | Теоретичне опитування.<br>Здача лабораторної роботи. | **10**<br><br>**10** |
| Тема 2. Захист від мережевих атак. | **2/2** | Дослідження класифікації мережевих атак та дослідження методів протидії і захисту. | Здача лабораторної роботи. | **10** |
| Тема 3. Забезпечення безпеки інформації у хмарних сервісах. | **2/2** | Дослідження моделей обслуговування у хмарних технологіях. | Здача лабораторної роботи. | **10** |
| Тема 4. Криптографія та інфраструктура відкритих ключів. | **2/2** | Дослідження методів хешування, шифрування, видів ключів та захищених з'єднань. | Здача лабораторної роботи. | **10** |
| Тема 5. Засоби віртуалізації. Типи. Принципи роботи. Засоби захисту. | **2/2** | Дослідження засобів віртуалізації та принципів їх роботи. | Здача лабораторної роботи. | **10** |
| Тема 7. Реагування на інциденти та їх обробка. | **2/2** | Дослідження систем реагування на інциденти інформаційної безпеки. | Здача лабораторної роботи. | **10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **30** |
| **Всього за семестр** | | | | **70** |

| | | |
|---|---|---|
| **Екзамен** | **Тест, теоретичні питання, задача** | **30** |
| **Всього за курс** | | **100** |

## ПОЛІТИКА ОЦІНЮВАННЯ

| | |
|---|---|
| ***Політика щодо дедлайнів та перескладання:*** | Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження). |
| ***Політика щодо академічної доброчесності:*** | Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). |
| ***Політика щодо відвідування:*** | Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету) |

## ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

| **Рейтинг здобувача вищої освіти, бали** | **Оцінка національна за результати складання екзаменів заліків** | |
|---|---|---|
| | **Екзаменів** | **Заліків** |
| 90-100 | Відмінно | зараховано |
| 74-89 | Добре | |
| 60-73 | Задовільно | |
| 0-59 | незадовільно | не зараховано |

### Рекомендовані джерела інформації


1. Зінченко О.В., Іщеряков С.М., Прокопов С.В., Сєрих С.О., Василенко В.В. Хмарні технології. – Навчальний посібник. – К: ФОП Гуляєва В.М., 2020. – 74 с.

2. Соколов В. Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.

3. Raghuram Yeluri, Enrique Castro-Leon. Building the Infrastructure for Cloud Security: A Solutions View. Apress, 2014 p. - 244 p.

4. Huseni Saboowala, Muhammad Abid, Sudhir Modali. Designing Networks and Services for the Cloud: Delivering business-grade cloud applications and services. Cisco Press, 2013. - 336 p.