



СИЛАБУС ДИСЦИПЛІНИ «ПРОДУКТИ ТА ПОСЛУГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 8
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу



Сагун Андрій Вікторович, к.т.н., доцент
([портфоліо](#))

Контактна інформація
лектора (e-mail)

Кафедра комп'ютерних систем, мереж та кібербезпеки
корпус. 15, к. 207, тел. 5278724
e-mail a.sagun@nubip.edu.ua
ЕНК (1 семестр)
<https://elearn.nubip.edu.ua>

Сторінка курсу в eLearn

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення практики проектування та використання продуктів та послуг інформаційної безпеки (ППІБ). В курсі розглядається підходи до проектування продуктів та послуг інформаційної безпеки, що пов'язані з неперервністю процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. Увагу приділено застосуванню національних та міжнародних регулюючих актів в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

Навчальна дисципліна забезпечує формування ряду загальний компетентностей:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

фахових компетентностей:

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 інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

У результаті вивчення навчальної дисципліни студент набере певні програмні результати, а саме:

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

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 рухаетесь за графіком навчання.

Неформальна on-line освіта на основі МВОК.

СТРУКТУРА КУРСУ

| Тема | Годин и (лекції/ лабора торні,) | Результати навчання | Завдання | Оціню вання |
|---|---|--|----------------------------|----------------|
| 1 семестр. | | | | |
| Модуль 1. Методики проектування та використання продуктів та послуг інформаційної безпеки | | | | |
| Етапи та алгоритми проектування ППБ. Методика синтезу ППБ на базі існуючих мережних компонент. | 2/- | Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих | Опитування | 2 |
| Завантаження та налаштування компонент ППБ та конфігураційних файлів. | 4/6 | процедур; Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. | Захист лабораторної роботи | 12 |
| Проектування та реалізація захищених каналів передачі на базі алгоритмів та вимог стандарту ДСТУ ISO/IEC 27033-5:2016 для VPN-мереж | 6/6 | | Здача лабораторної роботи. | 15 |
| Модульний контроль | | | Модульний тест в ЕНК | 6 |
| Всього за 1 модуль | 12/12 | | | 35 |
| Модуль 2. Проектування послуг інформаційної безпеки, пов'язаних з моніторингом та реагуванням на загрози серверних платформ | | | | |
| Проектування послуг реагування на потенційні загрози безпеці серверів на базі ОС Linux | 4/4 | Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих | Здача лабораторної роботи. | 9 |
| Проектування та реалізація ППБ мережевої ідентифікації на базі *nix | 4/4 | процедур; Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. | Здача лабораторної роботи. | 10 |
| Автоматизація обробки ведення журналів безпеки серверних ОС на базі ОС Linux | 4/4 | | Здача лабораторної роботи. | 10 |
| Модульний контроль | | | Модульний тест в ЕНК | 6 |
| Всього за модуль 2 | 12/12 | | | 35 |
| Екзамен | | | Підсумковий тест в ЕНК | 30 |
| Всього за курс | 24/24 | | | 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

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

Рекомендовані джерела інформації

1. Остапов С. Е. Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с. – URL: <http://kist.ntu.edu.ua/textPhD/tzi.pdf>
2. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. – URL: <https://er.nau.edu.ua/handle/NAU/32583>
3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р.
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
5. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 63.