СИЛАБУС ДИСЦИПЛІНИ «УПРАВЛІННЯ ДОСТУПОМ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма навчання денна
Кількість кредитів ЄКТС 4
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
Сторінка курсу в eLearn	**ЕНК (6 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4785

ОПИС ДИСЦИПЛІНИ

Сучасні інформаційні та комп'ютеризовані системи уразливі до ряду мережних загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття або модифікації інформації. Щоб захистити відповідні інформаційні ресурси від кіберзагроз, необхідно застосовувати цілеспрямовані заходи управління доступом. Вивченню та засвоєнню керівних та загальних принципів побудови, реалізації, підтримки та покращення системи керування доступом та захистом інформації присвячена ця дисципліна. Студенти здобувають практичні навички з планування та розроблення ефективної системи управління доступом, яка забезпечує керування й контроль доступу, розробку й обслуговування апаратно-програмних систем та мереж; керування безперервністю бізнес-процесів та оптимізацію управлінських процесів. Студенти навчаються ідентифікувати специфічні ризики порушення безпеки, які загрожують ресурсам організації та для яких оцінюють уразливість, ймовірність її виникнення та потенційний вплив; розробляти політику безпеки; здійснювати організацію керування активами й ресурсами з метою підвищення ефективності функціонування і захищеності комп'ютерних систем.

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):

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.

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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

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

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

РН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

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.

РН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

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/ Лабора-торні,)	Результати навчання	Завдання	Оціню-вання
6 семестр				
Змістовний модуль 1. Сутність управління доступом. Ідентифікація, автентифікація, авторизація.				
Тема 1. Розкриття сутності управління доступом. Ідентифікація, автентифікація, авторизація та підзвітність.	**2/4**	РН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. РН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. РН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. РН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**25**
Тема 2. Управління ідентифікацією. Роль каталогів в управлінні ідентифікацією. Управління веб-доступом. Управління паролями.	**2/4**			**25**

Тема 3. Управління обліковими записами. Ініціалізація користувача. Біометрія.	**2/4**	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.		**25**
Тема 4. Управління паролями. Когнітивні паролі. Одноразові паролі. Криптографічні ключі. Карти пам'яті. Смарт-карти.	**2/4**	РН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.		**25**
Змістовний модуль 2. Моделі, методи та засоби управління доступом.				
Тема 5. Моделі управління доступом.	**2/4**	РН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**25**
Тема 6. Техніки і технології управління доступом.	**2/4**	РН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.		**25**
Тема 7. Методи управління доступом. Рівні управління доступом. Типи управління доступом.	**2/4**	РН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.		**25**
Тема 8. Загрози управлінню доступом.	**2/2**	РН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). 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. РН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.		**25**
Всього за семестр				**0,7*(100 +100)/2 = 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 27.12.2019 р. № 1371):

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