СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Навчальна практика з проектування систем кібербезпеки»

Ступінь вищої освіти - Бакалавр
Спеціальність «125-Кібербезпека»
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 4
Форма здобуття вищої освіти - денна
Кількість кредитів ЄКТС 5
Мова викладання українська/англійська

Лектор навчальної дисципліни	 **Сагун Андрій Вікторович, к.т.н., доцент** **(портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем і мереж,** **корпус. 15, к. 207, тел. 5278724** **e-mail a.sagun@nubip.edu.ua**
URL ЕНК на навчальному порталі НУБіП України	**ЕНК (4 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=5066

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення дисципліни «**Навчальна практика з проектування систем кібербезпеки**» є вивчення технологій проектування систем захисту інформації в інформаційно-комунікаційних системах та мережах відповідно до вимог чинних нормативних документів.

Вивчаються принципи побудови захищених корпоративних мереж на базі технології Active Directory. Розглядаються основи планування та впровадження систем кібербезпеки на підприємствах різних форм бізнесу і діяльності, технології захисту конфіденційності, цілісності та доступності інформації з врахуванням існуючих моделей загроз і порушника.

Компетентності навчальної дисципліни:

Загальні:

- здатність застосовувати знання у практичних ситуаціях.
- знання та розуміння предметної області та розуміння професії.
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

- 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.
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
- здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
- здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

Програмні результати навчання навчальної дисципліни:

– застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

– використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

– адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

– критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

– діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

– розробляти моделі загроз та порушника;

– вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

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

– реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

– вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

– 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;

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

– застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

– вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

– приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

– вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

– вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для систем захисту інформації

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** (практичні)	**Результати навчання**	**Завдання**	**Оцінювання**
1 семестр				
Модуль 1. Планування та аналіз мережевих технологій для створення захищеної ІКС				
Тема 1. Визначення моделі загроз, порушника. Формування моделі захищеної корпоративної мережі підприємства	**15**	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; Розробляти моделі загроз та порушника; Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-		**2**
Тема 2. Аналіз та планування комунікаційної складової захищеної корпоративної мережі (КМ). Вибір середовищі моделювання та віртуалізації процесів захисту	**15**		Опитування	**2**
Тема 3. Визначення типу та рівня гарантування послуг безпеки функціонального профіля захищеності КМ за НД ТЗІ 2.4-005-99	**10**		Опитування	**2**
Тема 4. Визначення серверних ролей та компонент для забезпечення функціональності проектного рішення системи розмежування доступу до корпоративної інформації засобами	**8**		Опитування	**2**

Windows Server (враховуючи модель загроз).		телекомунікаційних (автоматизованих) системах;		
	2	Розробляти моделі загроз та порушника;	Здача звіту частини 1	**12**
Всього за модуль	**50**			**20**
Модуль 2. Проектування та реалізація технологій захисту інфраструктури корпоративної ІКС				
Тема 5. Планування та розгортання ефективної доменної структури КМ	**5**	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;	Опитування	**2**
Тема 6. Визначення користувачів та функціональних груп доступу до захищених ресурсів ІКС	**10**		Опитування.	**2**
Тема 7. Розробка механізмів авторизації та парольних політик користувачів корпоративної комп'ютерної мережі	**15**		Опитування	**2**
Тема 8. Організація захищених сховищ корпоративної інформації.. Проектування та реалізація RAID-масивів	**10**		Опитування	**2**
Тема 9. Проектування та організація системи розмежування доступу до корпоративних файлових ресурсів та периферійних пристроїв загального користування на базі технології AD	8		Опитування	**2**
	2		Здача звіту частини 2	**10**
Всього за модуль	**50**			**20**
Модуль 3. Проектування та застосування групових та корпоративних політик безпеки та систем розмежування доступу				
Тема 10. Налаштування механізмі корпоративної безпеки служби каталогів AD: об'єкти та групові політики для доступу в рамках корпоративної мережевої ОС. Групові та локальні політики доступу.	**20**	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для систем захисту інформації	Опитування	**2**
Тема 11. Механізми захисту корпоративних ресурсів з використанням технологій резервування та реплікації	**15**		Опитування	**2**
Тема 12. Налаштування корпоративного серверу електронної пошти на базі e-mail серверу MS Exchange. Проектування політик облікових поштових записів	**10**		Опитування	**2**
	5		Здача звіту частини 3	**14**
Всього за модуль	**50**			**30**
Залік			**Тест, теоретичні питання, задача**	**30**
Всього за курс	**150**			**100**

Неформальна on-line освіта на основі МВОК.

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). В разі здачі лабораторних робіт пізніше запланованих термінів без поважної причини оцінка може бути знижена
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв).
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	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Рекомендована література

1. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection [Edition : 2], 2013, 23 p. Access via: https://www.iso.org/ru/isoiec-27001-information-security.html
2. Закон «Про інформацію»: від 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України, 1992. – № 48. – С. 650.
3. Закон України «Про доступ до публічної інформації» // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text
4. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
5. Закон України «Про захист персональних даних» // Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
6. Закон України «Про основні засади забезпечення кібербезпеки України» //Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99. ДСТСЗІ СБ України, Київ. – 1999.
8. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». - 1999. Київ. – 22 с.
9. НД ТЗІ 2.6-002-2015. Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. ДСТСЗІ СБ України.

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Київ. – 2016.

10. А.В. Сагун, В.Б. Бобков. Операційні системи та комп'ютерні мережі [навчальний посібник] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Автоматизація та комп'ютерно-інтегровані технології кібер-енергетичних систем» спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», освітньо-професійною програмою / КПІ ім. Ігоря Сікорського ; уклад. А. В. Сагун. – Електронні текстові данні (1 файл 10 Мбайт). – Київ : КПІ ім. Ігоря Сікорського», 2021. – 164 с. – Назва з екрана.