ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС (SYLLABUS)
Дисципліна «Основи кібербезпеки/Cybersecurity essentials»

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

Викладач	Савченко Тетяна Віталіївна
Науковий ступінь	Кандидат технічних наук
Вчене звання	Доцент
Посада	Доцент кафедри інженерії програмного забезпечення та кібербезпеки
Адреса кафедри	м. Київ, вул. Кіото 19, каб. Б-531, Б-524
E-mail	progen@ukr.net
Консультації	Відповідно до графіку індивідуальних консультацій на сайті кафедри

ПОЛІТИКА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

https://knute.edu.ua/file/MzEyMQ==/c12a9f74e87d9154696ca0f761da2e5c.pdf

Дотримання академічної доброчесності студентами передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

- академічний плагіат – оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів

власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

- самоплагіат – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;
- фабрикація – вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;
- фальсифікація – свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;
- списування – виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (модульний контроль, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньо-професійної програми;
- відрахування з Університету;
- позбавлення наданих університетом пільг;
- відмова у присудженні відповідного ступеня вищої освіти;

ПОЛІТИКА ЩОДО ВІДВІДУВАННЯ ЗАНЯТЬ

- відвідування занять є обов'язковим;
- за об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із викладачем дисципліни.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва дисципліни/ тип дисципліни	Основи кібербезпеки / вибіркова
Навчальний рік	2023/2024
Факультет	Факультет інформаційних технологій
Курс	3-4
Семестр	6-8
Освітній ступінь	бакалавр
Галузь знань	12 «Інформаційні технології»
Спеціельність	126 «Інформаційні системи і технології»

Загальна характеристика	Кількість годин –180 Кількість кредитів – 6 **Співвідношення аудиторних годин і годин самостійної роботи** - 40/140 **Мова викладання** – українська **Форма викладання** – очна
Програмне забезпечення	Глобальна мережа Інтернет, локальна комп'ютерна мережа, антивірусні програми..
Обладнання	Проектор, комп'ютерна техніка із встановленим програмним забезпеченням та доступом до мережі Інтернет.
Необхідні попередні дисципліни	«Основи теорії інформаційних систем», «Інформаційні системи і технології»
Методика вивчення	Методика вивчення дисципліни полягає у набутті студентами знань загальнотеоретичного і практично-прикладного характеру під час лекцій, практичних занять, самостійної роботи та вивчення першоджерел і навчально-методичної літератури.
Мета і завлання	**Метою** дисципліни «Основи кібербезпеки» є формування у майбутніх фахівців необхідного рівня знань щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в професійній діяльності. дізнатись про основні загрози в сучасному інформаційному просторі; аналізувати поширені помилки користувачів та наслідки від атак зловмисників і кібершахраїв; вивчити базові правила захисту інформації на персональних електронних пристроях та в соціальних мережах; навчитись визначати фейкові новини; опанувати основні рекомендації щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами. **Завданням** вивчення дисципліни «Основи кібербезпеки» є засвоєння студентами: □ знання основних положень, термінів та заходів, що стосуються кібергігієни на робочу місці; □ знання основної нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки; □ знання особливостей кібергігієни в системі публічної служби. □ уміння визначати заходи кібергігієни для конкретної ситуації;

	уміння оцінювати загрози та вживати заходів реагування на робочому місці; уміння безпечно поводитись у кіберсфері. навички організації безпечного доступу до пристроїв і програм; навички правильного налаштування програмного забезпечення на робочому місці; навички критичного оцінювання інформації; знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей, тощо..
Місце дисципліни в освітньо-професійній програмі	
Загальні компетентності	КЗ 2. Здатність застосовувати знання у практичних ситуаціях.
Фахові компетентності (результати навчання)	КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.
Програмні результати навчання	ПР 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ТЕМАТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації

Поняття інформаційна безпека, кібербезпека, кіберпростір, кібероборотьба, кібертероризм, кіберзброя. Кіберпростір як сфера ведення війн сучасності та майбутнього. Сутність кібербезпеки інформаційного суспільства. Кіберінциденти: передумови скоєння та наслідки. Дії у кіберпросторі та їх особливості. Класифікація форм і способів кібердій. Основи кіберрозвідки. Основи кіберзахисту. Огляд областей кібербезпеки. Приклади доменів кібербезпеки. Зростання кібер-доменів. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників.

Тема 2. Національна система кібербезпеки України

Основні положення Стратегії кібербезпеки України. Сутність та завдання Національної системи забезпечення кібербезпеки України Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством. Захист відкритої інформації в державних органах. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. Структура національної безпеки України. Суб'єкти забезпечення інформаційної безпеки як складової національної безпеки України. Основні пріоритети забезпечення інформаційної безпеки.

Тема 3. Сутність та основні процедури керування кібербезпекою

Модель кібербезпеки ISO. Огляд моделі. Галузі кібербезпеки. Цілі контролю. Контроль. Використання моделі ISO для кібербезпеки. Модель кібербезпеки ISO та тріада КЦД. Модель кібербезпеки ISO і можливі стани даних. Модель кібербезпеки ISO і технології захисту.

Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак

Комп'ютерні атаки та технології їхнього виявлення. Сутність та класифікація кібератак. Етапи реалізації атак. Відмова в обслуговуванні. Аналіз трафіку (Sniffing). Підміна. Man-in-the-middle. Атаки нульового дня. Клавіатурні шпигуни (кейлогери). Захист від атак. Атаки на бездротові мережі та мобільні пристрої. Grayware та SMiShing. Несанкціоновані точки доступу. Глушіння радіочастот (RF Jamming). Bluejacking та Bluesnarfing. Атаки на WEP та WPA. Захист від атак на бездротові мережі та мобільні пристрої. Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. Захист від атак на застосунки. Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS). Отруєння SEO. Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Внутрішні та зовнішні кіберзагрози. Кіберзагрози через Інтернет-сервіси. Поширення кіберзагроз. Кіберзагрози підвищеної складності.

Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії

Поняття «дезінформації». Канали поширення дезінформації. Типи неправдивої інформації. Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень. Види маніпуляцій. Маніпуляції з медіаданими. Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень.

Пропаганда як інструментів інформаційного впливу. Способи протидії неправдивим повідомленням.

Тема 6. Комп'ютерна вірусологія

Загальні поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження. Класифікація комп'ютерних вірусів і принципи її побудови. Алгоритми роботи вірусів. Файлові, завантажувальні (бутові) та файлово-завантажувальні віруси. Макровіруси та мережні віруси. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів. Шляхи розповсюдження шкідливого програмного забезпечення (ШПЗ), вектори атак. Типи шкідливого програмного забезпечення. Шпигунські програми (spyware). Симптоми зараження ШПЗ. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger "кейлогер". «JS-сніфери». Троянські програми віддаленого доступу .rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-шантажист). Майнери (miners). Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення. Рекламне шкідливе програмне забезпечення (adware).

Тема 7. Соціальна інженерія

Поняття соціальної інженерії. Методи соціальної інженерії. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). Фішингова атака. Етапи атаки із використанням СІ. Розвідка та збір інформації із відкритих джерел. Легендування та планування атаки із використання методів СІ. Використання вразливостей як розповсюджений метод проникнення для отримання інформації.

Тема 8. Соціотехнічна безпека: проблемні аспекти

Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем: основні аспекти, поняття та визначення. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.

Тема 9. Безпека спілкування в кіберпросторі

Захист інформації в глобальних мережах. Характер проведення атак у глобальних мережах. Захист під час використання WWW (World Wide Web). Безпечне користування мережею «Інтернет». Найпоширеніші способи нелегального заробітку в мережі «Інтернет». Безпека браузерів. Безпека даних. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI. Безпечне користування месенджерами.

Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі

Безпека користування соціальними мережами. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки. Безпека мобільних пристроїв. Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями. Безпека користування електронною поштою. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи (investigation). Забезпечення безпеки особистої поштової скриньки (рекомендації).

Тема 11. Безпека цифрового простору суб'єктів господарювання

Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку. Класифікація каналів витоку інформації. Методи та засоби блокування технічних каналів витоку інформації. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Захист акустичної інформації від зняття радіопристроями. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.

Тема 12. Безпека Інтернету-речей

Історія Інтернету-речей. Екосистема Інтернету-речей. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок». Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології. Криптографія. Симетрична криптографія. Асиметрична криптографія. Криптографічний хеш (аутентифікація і цифровий підпис).

Інфраструктура відкритого ключа. Блокчейн і криптовалюта в Інтернеті-речей. Рекомендації щодо захисту IoT-пристроїв.

Тема 13. Системи захисту інформації на проникнення

Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту. Фізична безпека. Загрози, пов'язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet. Захист інформації за допомогою міжмережних екранів. Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Історичні приклади стеганосистем. Галузі застосування стеганографії. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. Практичні аспекти побудови стеганосистем. Приховування даних у текстових файлах: методи текстової стеганографії; аналіз реалізації методів.

Тема 14. Основні методи забезпечення кібербезпеки суб'єкта господарювання

Типи контролю доступу. Контроль фізичного доступу. Системи розмежування логічного доступу. Адміністративний контроль доступу. Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил. Ідентифікація. Управління ідентифікацією та доступом. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація. Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Авторизація. Використання авторизації. Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Ефективні механізми розкриття порушень. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю. Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів. Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень. Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму.

Перелік навчальних робіт студентів та оцінки їх у балах з дисципліни «Основи кібербезпеки»

Назва теми	Кількість годин				Форми контролю
	Усього год/кре	Лекції	Лабо-раторні	Самос-тійна	

	дитів		заняття / МК	робота студ.	
Тема 1. Кіберпростір і кібербезпека ─ головні ознаки нової інформаційної цивілізації	13	2	2	10	К, ЛР, ПСР
Тема 2. Національна система кібербезпеки України	13		2	10	К, ЛР, ПСР
Тема 3. Сутність та основні процедури керування кібербезпекою	13	2	2	10	К, ЛР, ПСР
Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак	12	2		10	К, ЛР, ПСР
Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії	13		2	10	К, ЛР, ПСР
Тема 6. Комп'ютерна вірусологія	14	2	2	10	К, ЛР, ПСР
Тема 7. Соціальна інженерія	12	2	2	10	К, ЛР, ПСР
Тема 8. Соціотехнічна безпека: проблемні аспекти	12			10	К, ЛР, ПСР
Тема 9. Безпека спілкування в кіберпросторі	14	2	2	10	К, ЛР, ПСР
Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі	13	2	2	10	К, ЛР, ПСР
Тема 11. Безпека цифрового простору суб'єктів господарювання	12		2	10	К, ЛР, ПСР
Тема 12. Безпека Інтернету-речей	13	2		10	К, ЛР, ПСР
Тема 13. Системи захисту інформації на проникнення	13	2	2	10	К, ЛР, ПСР
Тема 14. Основні методи забезпечення кібербезпеки суб'єкта господарювання	13	2		10	К, Т, ЛР, ПСР, ПК
Разом	180/6	20	20	140	
Підсумковий контроль – екзамен					

Примітка: Т – тестування; ЛР – захист лабораторних робіт; ПСР – перевірка самостійної роботи; ПК - підсумковий контроль; К – конспект.

КОНТРОЛЬ ТА КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

При вивченні дисципліни використовуються наступні форми контролю знань студентів: поточний; модульний; підсумковий.

Поточний контроль передбачає перевірку теоретичних питань, самостійної роботи, практичних робіт та усне опитування по кожній практичній

роботі. По даному виду контролю оцінювання знань студентів здійснюється у відповідності до бального розподілу наведеного в попередній таблиці.

Формою підсумкового контролю є екзамен. Екзаменаційна оцінка (100 балів) є результатом виконання двох теоретичних питань (2 х 30 балів = 60 балів) та практичного завдання (40 балів).

Результуюча оцінка з дисципліни визначається як середня від балів набраних протягом семестру та отриманих на іспиті.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний:

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8
2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.− К.: ДУТ, 2015.− 288 с.
3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.
4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.