



СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ БЕЗПЕКА ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	Вибіркова компонента освітніх програм першого (бакалаврський) рівня вищої освіти
Рекомендовано для спеціальностей	Для всіх ОПП запроваджених ДУІТЗ
Форма навчання	Денна, заочна

Викладачі

Севастьян Євген Олександрович
seva.odessa@gmail.com



Старший викладач кафедри Кібербезпеки та
технічного захисту інформації

Загальна інформація про дисципліну

Анотація до дисципліни

Дисципліна присвячена основам забезпечення безпеки в системах електронного документообігу. Розглядаються методи захисту конфіденційності, цілісності та доступності документів, управління доступом до даних, аналіз загроз та ризиків. У курсі вивчаються сучасні підходи до побудови політик інформаційної безпеки та впровадження практичних рішень для захисту електронного документообігу в організаціях.

Мета дисципліни	формування знань щодо застосування методів та засобів забезпечення безпеки електронного документообігу, оволодіння технологіями ідентифікації загроз та вибору стратегій захисту залежно від типу документів і процесів, розуміння комп'ютерних технологій управління доступом і моніторингу активності, а також оптимальних інструментів для захисту інформації в системах електронного документообігу.
Компетентності, формуванню яких сприяє дисципліна	Здатність застосовувати знання у практичних ситуаціях. Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
Результати навчання	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
Обсяг дисципліни	Загальний обсяг дисципліни 6 кредитів ЄКТС (180 академічних годин)
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркового компонент освітньої програми

Програма дисципліни

Тема 1.	<i>Вступ до електронного документообігу</i> Основні поняття та структура систем електронного документообігу. Сфери застосування та переваги електронного документообігу. Правові аспекти впровадження та використання систем ЕДО.
Тема 2.	<i>Загрози та ризики в системах електронного документообігу</i> Основні типи загроз: несанкціонований доступ, втрати даних, зловживання правами доступу. Ризики для бізнесу та організацій при використанні ЕДО. Методи оцінки ризиків.
Тема 3.	<i>Основи управління доступом</i> Методи управління доступом до документів та даних. Моделі контролю доступу (RBAC, DAC, MAC). Принципи мінімальних привілеїв та сегментації даних.
Тема 4.	<i>Моніторинг та аудит в системах ЕДО</i> Інструменти моніторингу діяльності користувачів. Аналіз логів та слідів доступу. Проведення аудитів безпеки в системах ЕДО.
Тема 5.	<i>Технології забезпечення безпеки даних</i> Методи забезпечення цілісності та конфіденційності даних. Використання резервного копіювання, контроль версій документів. Забезпечення доступності документів в умовах інцидентів.

Тема 6.	Аналіз інцидентів у системах ЕДО Методи ідентифікації та реагування на інциденти безпеки. Виявлення порушень безпеки, аналіз дій зловмисників. Побудова плану відновлення після інцидентів.
Тема 7.	Правові аспекти та регулювання ЕДО Основні нормативно-правові акти України та міжнародні стандарти, що регулюють електронний документообіг. Особливості дотримання норм GDPR, ISO 27001 та інших стандартів.
Тема 8.	Використання сучасних інструментів безпеки для ЕДО Огляд програмного забезпечення для моніторингу, управління доступом та захисту даних у системах ЕДО. Приклади впровадження у реальних організаціях.

Список рекомендованих джерел

1. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson.
2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
3. Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.
4. Shon Harris, F., & Maymi, F. (2021). *CISSP All-in-One Exam Guide*. McGraw Hill.
5. Solomon, M. (2011). *Security Policies and Implementation Issues*. Jones & Bartlett Learning.

Інформація про консультації

Індивідуальні та колективні консультації проводяться в час, визначений за попередньою домовленістю з викладачем через засоби зв'язку.

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою		Нарахування балів	Бали нараховуються таким чином:
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано		Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну до 60 балів, за результати індивідуального завдання – до 40 балів. При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		

0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		
------	---	--	---	--	--

Політика опанування дисципліни

Відвідування:

Відвідування та відпрацювання пропущених занять є обов'язковим. Допускаються пропуски занять з поважних причин, які підтверджуються документально. За такої умови навчання може відбуватися в режимі он-лайн за погодженням із деканатом.

Дотримання принципів академічної доброчесності:

Політика щодо академічної доброчесності побудована на основі «Положення про академічну доброчесність» в університеті. Списування під час виконання письмових контрольних видів робіт заборонено. Користуватися мобільними пристроями, під час проведення різних видів контролю успішності, дозволяється лише з дозволу викладача.

Умови зарахування пропущених занять:

Відпрацювання пропущених занять проходять в дні згідно графіку консультацій викладачів кафедри.