СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КІБЕРБЕЗПЕКА ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ»

Спеціальність	*D4 Публічне управління та адміністрування*
Освітньо-професійна програма	*«Публічне управління та адміністрування в умовах кризового менеджменту і реформ»*
Освітній рівень	*Другий (магістерський)*
Статус дисципліни	*Вибіркова (ВК 8)*
Мова викладання	*Українська*
Курс / семестр	*1 курс, 2-й семестр*
Кількість кредитів ЄКТС	*4*
Розподіл за видами занять та годинами	*Денна: лекції - 20 год., семінарські/практичні - 20 год., самостійна робота - 80 год.* *Заочна: лекції - 8 год., семінарські/практичні - 4 год., самостійна робота - 108 год.*
Форма підсумкового контролю	*Диференційований залік*
Викладач	*Карташов Є.М., доктор наук з державного управління, професор кафедри публічного управління та адміністрування*
Консультації	*За розкладом та за домовленістю; дистанційні (Zoom / Teams); індивідуальні або групові*

Мета навчальної дисципліни

Формування у здобувачів магістерського рівня здатності до розуміння сучасних кіберзагроз для державних інформаційних систем та КІІ; застосування правових засад і стандартів (ISO 27001, NIST CSF, стандарти НАТО) кіберзахисту; формування та реалізації політики кібербезпеки в органах публічної влади; реагування на кіберінциденти, розробки BCP/DRP; організації кіберосвіти державних службовців. Підготовка управлінця-практика, здатного координувати кіберзахист органу влади та приймати рішення під час кібератак.

Передумови для навчання

Базові знання з ІКТ та інформаційної безпеки. Рекомендовано: ВК2 «Державні комунікаційні системи управління», ВК6 «Документообіг в державній службі».

Зміст навчальної дисципліни
Тема 1. Основи кібербезпеки: поняття, загрози, вразливості, ризики
Тема 2. Державна система кібербезпеки України: структура, повноваження, законодавство
Тема 3. Міжнародні стандарти кібербезпеки: ISO 27001, NIST CSF, стандарти НАТО
Тема 4. Кіберзагрози для органів публічної влади: APT, фішинг, DDoS, ransomware
Тема 5. Організація захисту державних реєстрів, баз даних та систем електронного урядування
Тема 6. Управління інцидентами кібербезпеки: CSIRT/CERT, процедури реагування
Тема 7. Планування безперервності (BCP) та відновлення після аварій (DRP) в органах влади
Тема 8. Кібербезпека в умовах воєнного стану: досвід України 2022-2025
Тема 9. Кіберосвіта та кібергігієна державних службовців: як подолати людський фактор
Тема 10. Інтегративний кейс-тренінг: реагування на кібератаку на орган державної влади

Сторінка курсу на платформі Moodle	Матеріали курсу (РПНД, силабус, звіти CERT-UA, шаблони BCP/DRP, тести): https://kuait.eu/moodle/course/index.php?categoryid=39

Рекомендовані джерела

Нормативні:
1. Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII.
2. Стратегія кібербезпеки України (2021, оновлення 2023).
3. ISO/IEC 27001:2022. Information security management systems.
4. NIST CSF v1.1 (Framework for Improving Critical Infrastructure Cybersecurity).
Основні:
5. Комаров О.О. Кібербезпека в публічному управлінні. - К.: НАДУ, 2023.
6. CERT-UA. Щорічний звіт про кіберінциденти (2024, 2025): https://cert.gov.ua
Додаткові:
7. ENISA Threat Landscape Report 2024.
8. NATO CCDCOE. Tallinn Manual 3.0. - Tallinn, 2024.

Інформаційні ресурси

CERT-UA: https://cert.gov.ua
Держспецзв'язку: https://cip.gov.ua
НКЦК: https://ncscc.gov.ua
ENISA: https://www.enisa.europa.eu
NIST CSF: https://www.nist.gov/cyberframework

Система оцінювання результатів навчання

Поточний контроль:
1. Аналітична довідка «Кіберзагрози для держ. ІС України 2024-2025» - 15 балів (15%)
2. Правовий аналіз: обов'язки органу влади щодо повідомлення про кіберінцидент - 10 балів (10%)
3. Розробка Security Awareness Program для державних службовців - 15 балів (15%)
4. Командна ділова гра «Реагування на кібератаку» (індив. оцінка) - 20 балів (20%)
5. Підсумковий диференційований залік - 40 балів (40%)
Мінімум для допуску до заліку - 60 балів.
Детальні критерії оцінювання наведено в РПНД.

Шкала оцінювання (ЄКТС)

90-100 (A) - відмінно / зараховано
82-89 (B), 74-81 (C) - добре / зараховано
64-73 (D), 60-63 (E) - задовільно / зараховано
35-59 (FX) - незадовільно з можливістю перескладання / не зараховано
0-34 (F) - незадовільно з обов'язковим повторним вивченням / не зараховано

Політики навчальної дисципліни

Оригінальність письмових робіт - мінімум 80%; посилання на звіти CERT-UA, законодавство та стандарти ISO/NIST є обов'язковими. Аналітична довідка, правовий аналіз та Security Awareness Program виконуються індивідуально. Ділова гра - командна з фіксацією внеску. Відповідальність за фальсифікацію даних - оцінка 0 балів та направлення до Комісії КУАІТ.

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання та форм оцінювання наведено у Робочій програмі навчальної дисципліни (https://kuait.eu/moodle/course/index.php?categoryid=39).

Київський університет авіаційних та інформаційних технологій

Силабус затверджено
на засіданні кафедри публічного управління та адміністрування

Протокол № 4 від 05.11.2025 р.

Завідувач кафедри:  О.М. Непомнящий