СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СТАНДАРТИ ТА ПОЛІТИКИ КІБЕРБЕЗПЕКИ»

Компонента освітньої програми – ***вибіркова*** (*3 кредити*)

Освітньо-професійна програма	Комп'ютерна інженерія
Спеціальність	F7 Комп'ютерна інженерія
Галузь знань	F Інформаційні технології
Рівень вищої освіти	другий (магістерський)
Мова навчання	українська
Профайл викладача	Іванущак Наталія Михайлівна, асистент, кандидат технічних наук https://csn.chnu.edu.ua/employees/ivanushhak-nataliya-myhajlivna/
Контактний тел.	+(38) 0372 50 94 32 (кафедра КСМ) – Іванущак Н.М.
E-mail:	n.ivanuschak@chnu.edu.ua
Сторінка курсу в Moodle	https://moodle.chnu.edu.ua/course/view.php?id=1561
Консультації	*Очні консультації*: за попередньою домовленістю. *Онлайн-консультації*: згідно погодженого графіку

АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Стандарти та політики кібербезпеки» спрямована на формування системи знань про нормативно-правові засади, міжнародні стандарти та організаційно-технічні механізми забезпечення кібербезпеки підприємств, установ і організацій. У межах дисципліни розглядаються законодавство України у сфері кібербезпеки, принципи цифрової етики, вимоги щодо захисту персональних даних, фреймворк NIST Cybersecurity Framework і CIS Controls.

Особлива увага приділяється розробленню, упровадженню та супроводу внутрішніх політик інформаційної безпеки, управлінню ризиками кібербезпеки, оцінюванню відповідності встановленим вимогам, проведенню аудиту та організації реагування на інциденти кібербезпеки. Вивчення дисципліни передбачає ознайомлення з методами ідентифікації загроз, оцінювання ефективності заходів захисту інформації та формування організаційних механізмів контролю дотримання вимог безпеки.

Опрацювання дисципліни сприяє формуванню компетентностей, необхідних для аналізу нормативних вимог, вибору відповідних стандартів, розроблення політик кібербезпеки та забезпечення їх практичного застосування в інформаційних системах організацій.

Метою навчальної дисципліни є формування у здобувачів вищої освіти знань і практичних навичок щодо застосування нормативно-правових вимог, міжнародних

стандартів і рекомендацій у сфері кібербезпеки, розроблення та впровадження внутрішніх політик інформаційної безпеки, управління ризиками, оцінювання відповідності вимогам безпеки та організації контролю ефективності заходів кіберзахисту.

Завдання вивчення навчальної дисципліни

Основними завданнями вивчення дисципліни є:

1. Вивчення нормативно-правової бази України у сфері кібербезпеки, захисту інформації та регулювання інформаційних відносин.
2. Ознайомлення з принципами цифрової етики, правовими й організаційними аспектами захисту персональних даних та відповідального використання цифрових технологій.
3. Вивчення структури, принципів і практичних особливостей застосування NIST Cybersecurity Framework та CIS Controls для організації й удосконалення кіберзахисту.
4. Формування навичок розроблення внутрішніх політик і процедур інформаційної безпеки з урахуванням специфіки діяльності організації, її інформаційних ресурсів і вимог нормативних документів.
5. Засвоєння методів ідентифікації загроз, оцінювання ризиків інформаційної безпеки, визначення пріоритетів захисту та вибору заходів оброблення ризиків.
6. Ознайомлення з методами проведення аудиту кібербезпеки, оцінювання відповідності вимогам стандартів і внутрішніх політик, а також визначення ефективності впроваджених заходів захисту.
7. Вивчення принципів організації моніторингу дотримання політик кібербезпеки, документування порушень, реагування на інциденти та впровадження коригувальних заходів.
8. Формування здатності аналізувати стан кібербезпеки організації, обґрунтовувати вибір стандартів і заходів захисту та розробляти рекомендації щодо вдосконалення системи управління інформаційною безпекою.
9. Розвиток навичок практичного застосування нормативних документів, міжнародних стандартів і методичних рекомендацій для розв'язання типових завдань у сфері управління кібербезпекою.

НАВЧАЛЬНИЙ КОНТЕНТ ОСВІТНЬОЇ КОМПОНЕНТИ

МОДУЛЬ 1. НОРМАТИВНО-ПРАВОВІ ТА МІЖНАРОДНІ СТАНДАРТИ КІБЕРБЕЗПЕКИ	
Тема 1	Нормативно-правова база України в галузі кібербезпеки.
Тема 2	Цифрова етика та захист персональних даних.
Тема 3	Стандарти NIST Cybersecurity Framework та CIS Controls.
МОДУЛЬ 2. ПОЛІТИКИ КІБЕРБЕЗПЕКИ ТА УПРАВЛІННЯ РИЗИКАМИ	
Тема 4	Розроблення внутрішніх політик підприємства.
Тема 5	Управління ризиками інформаційної безпеки
Тема 6	Оцінювання відповідності вимогам кібербезпеки (Compliance)
Тема 7	Аудит кібербезпеки, моніторинг дотримання політик і реагування на інциденти.

ФОРМИ, МЕТОДИ ТА ОСВІТНІ ТЕХНОЛОГІЇ НАВЧАННЯ

Основними формами організації навчання є лекційні та лабораторні заняття, а також самостійна робота здобувачів вищої освіти. Самостійна робота спрямована на опрацювання матеріалів лекцій та літературних джерел. У процесі вивчення дисципліни застосовуються пояснювально-ілюстративний, демонстраційний, практичний і проблемно-пошуковий методи навчання, аналіз практичних ситуацій, обговорення, дискусії та презентація результатів виконаних завдань.

Застосовуються інноваційні освітні технології, зокрема, інформаційно-комунікаційні та студентоцентрованого навчання. Освітні технології передбачають використання мультимедійних матеріалів для лекційних занять, методичних вказівок для виконання лабораторних робіт, мов та середовищ розробки комп'ютерних програм, комп'ютерної та телекомунікаційної техніки, відеоконференцій, системи електронного навчання Moodle з метою розвитку навичок аналізу, розробки та використання комп'ютерних систем штучного інтелекту.

ФОРМИ Й МЕТОДИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ

***Поточний контроль*:** *усне опитування* студента на лекційних заняттях (фронтальне, індивідуальне); *письмовий контроль* (звіти із виконання лабораторних робіт); *практичний контроль* (захист лабораторних робіт).

Рубіжний контроль: тестовий контроль у кінці змістових модулів №1 і №2.

Підсумковий контроль – залік.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання програмних результатів навчання здобувачів освіти здійснюється за шкалою європейської кредитно-трансферної системи (ECTS). Критерієм успішного оцінювання є досягнення здобувачем вищої освіти мінімальних порогових рівнів (балів) за кожним запланованим результатом навчання.

ПОЛІТИКА ЩОДО АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ЧНУ:

- «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/etychnyi-kodeks-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/
- «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-zapobihannia-akademichnomu-plahiatu-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/
- «Політика використання штучного інтелекту в Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polityka-vykorystannia-shtuchnoho-intelektu-v-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/

Використання здобувачами освіти інструментів штучного інтелекту (ШІ) під час виконання навчальних завдань:

- допускається за умови дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої роботи, а у разі використання ШІ зобов'язаний зазначити факт і спосіб його застосування);
- не допускається використання ШІ як заміни самостійного виконання завдань або з метою порушення вимог академічної доброчесності;
- додаткові обмеження чи вимоги щодо використання ШІ можуть визначатися викладачем в освітньому процесі для конкретних видів навчальної діяльності відповідно до особливостей дисципліни.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Система електронного навчання Чернівецького національного університету імені Юрія Федьковича (Moodle). URL: https://moodle.chnu.edu.ua/
2. Законодавство України у сфері кібербезпеки та захисту інформації. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19.
3. Законодавство України про захист персональних даних. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.
4. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework.
5. CIS Critical Security Controls v8.1. Center for Internet Security. URL: https://www.cisecurity.org/controls.
6. 10. CERT-UA. Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/.
7. OWASP. OWASP Top 10: The Ten Most Critical Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/.
8. Center for Internet Security. CIS Critical Security Controls Navigator. URL: https://www.cisecurity.org/controls/cis-controls-navigator.
9. SANS Institute. Information Security Policy Templates. URL: https://www.sans.org/information-security-policy/.

Покликання на робочу програму навчальної дисципліни

https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/sylabusy-vybirkovyh-dystsyplin/