	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ Кафедра економіки, менеджменту та комерційної діяльності СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	

Назва курсу	УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ІТ СФЕРІ
Викладач	Рябоволик Тетяна Федорівна, кандидат економічних наук, доцент кафедри економіки, менеджменту та комерційної діяльності
Контактний телефон	+380500871913
E-mail	ryabovolik@ukr.net
Обсяг та ознаки дисципліни	Вибіркова дисципліна, змістових модулів – 3. Форма контролю: залік. Загальна кількість кредитів – 4, годин – 120. Формат: очний (offline / face to face) / дистанційний (online). Мова викладання: українська
Консультації	Консультації проводяться відповідно до графіку, розміщеному в інформаційному ресурсі moodle.kntu.kr.ua; у режимі відео конференцій Zoom, через електронну пошту, Viber, Telegram за домовленістю.
Пререквізити	Особливі вимоги відсутні

1. Мета і завдання дисципліни

Метою вивчення навчальної дисципліни "Управління інформаційною безпекою в ІТ сфері" є формування у студентів знань, навичок та вмінь, необхідних для ефективного управління процесами забезпечення інформаційної безпеки в організаціях. Це включає розуміння сучасних загроз інформаційній безпеці, методів захисту даних, політик безпеки, а також впровадження процедур і технологій для запобігання, виявлення та реагування на інциденти безпеки.

Завданням вивчення дисципліни є:

У межах курсу здобувачі вищої освіти продовжують формувати інтегральну, загальні та професійні компетентності, а саме: ознайомлюються з принципами та стандартами інформаційної безпеки; розвивають навички аналізу ризиків і управління ними; вивчають методи захисту інформації, включаючи криптографію, контроль доступу, моніторинг і аудит безпеки; навчаються розробці політик та процедур інформаційної безпеки; формують розуміння юридичних і етичних аспектів управління інформаційною безпекою.

2. Результати навчання

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати:

- основи інформаційної безпеки, ключові принципи та стандарти (ISO/IEC 27001, NIST);
- типи загроз та вразливостей інформаційних систем;
- методи та засоби захисту інформації, включаючи криптографію, автентифікацію та управління доступом;
- основи управління ризиками інформаційної безпеки;
- політики, процедури та нормативно-правові акти у сфері інформаційної безпеки;
- методи моніторингу, виявлення та реагування на інциденти безпеки;
- юридичні та етичні аспекти захисту інформації.

вміти:

- ідентифікувати та аналізувати загрози інформаційній безпеці;
- розробляти та впроваджувати політики і процедури інформаційної безпеки;
- здійснювати оцінку ризиків і застосовувати відповідні заходи для їх зниження.
- використовувати засоби криптографічного захисту даних;
- налаштовувати системи контролю доступу та управління привілеями користувачів.
- організовувати моніторинг інформаційної інфраструктури для виявлення інцидентів безпеки.
- розробляти плани дій при інцидентах і забезпечувати безперервність бізнес-процесів.

набути соціальних навичок(soft-skills):

- здійснювати професійну комунікацію IT-індустрії;
- ефективно пояснювати і презентувати матеріал;
- працювати в команді діяльності та виділяти авторський внесок;
- взаємодіяти в професійному IT-середовищі з питань інформаційної безпеки та комерційної таємниці.

3. Політика курсу та академічна доброчесність

Очікується, що здобувачі вищої освіти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті здобувачі вищої освіти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення вибіркових навчальних дисциплін та формування індивідуального навчального плану ЗВО; Кодексу академічної доброчесності ЦНТУ.

4. Програма навчальної дисципліни

Змістовий модуль 1. Теоретичні засади менеджменту інформаційної безпеки в ІТ сфері

Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки.

Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки.

Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки.

Тема 4. Роботи спеціалізованих міжнародних ІТ-організацій та об'єднань в галузі інформаційної безпеки.

Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.

Змістовий модуль 2. Практичні засади управління інформаційною безпекою в ІТ сфері

Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США

Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України

Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту)

Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)

Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки

Змістовний модуль 3. Політика та моніторинг інформаційної безпеки в ІТ-сфері

Тема 11. Зміст деталізованої політики безпеки

Тема 12. Департамент інформаційної безпеки і робота з персоналом

Тема 13. Організація реагування на надзвичайні ситуації (інциденти).

Тема 14. Аудит стану інформаційної безпеки на підприємстві.

Тема 15. Надання послуг у сфері інформаційної безпеки.

Тема 16. Надання послуг у сфері інформаційної безпеки (страхування).

Тема 17. Міжнародний стандарт ISO/IEC 27001.

Тема 18. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей.

5. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю здобувачів, усне опитування, письмовий контроль.

Рейтинг студента із засвоєння дисципліни визначається за 100 бальною шкалою, у тому числі: перший рубіжний контроль – 50 балів, другий рубіжний контроль – 50 балів.

Семестровий залік полягає в оцінці рівня засвоєння здобувачем вищої освіти навчального матеріалу на лекційних та практичних заняттях і виконання індивідуальних завдань за стобальною та дворівневою («зараховано», «не зараховано») та шкалою ЄКТС результатів навчання.

6. Рекомендована література

Основна

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с. URL: http://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик. URL: http://www.justinian.com.ua/article.php?id=3222

3. Закон України «Про інформацію» URL: https://zakon.rada.gov.ua/laws/show/2657-12

4. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р., URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

6. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.

7. Букет Д.А. Управління інформаційною безпекою за допомогою комплексної системи захисту. (2022) URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2617

8. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.

9. Поворознюк О.А. Багатокритеріальна оцінка альтернатив при проєктуванні двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації / А.І. Поворознюк, О.А. Поворознюк, Г.Є. Філатова // Системи управління, навігації та зв'язку, 2021 – вип. 2(64) – С.92-95.

10. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 346 с. URL: https://nasbu.edu.ua/uploads/p_57_53218641.pdf

Додаткова

1. Susukailo, V., Opirsky, I., Yaremko, O. (2021). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. У Lecture Notes in Electrical Engineering (с. 257–271). Springer International Publishing. URL: https://doi.org/10.1007/978-3-030-92435-5_15

2. Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32.

3. (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html

4. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/82875.html

5. (2013) ISO/IEC 27001: Information Technology — Security Techniques — Information Security Management Systems — Requirements. URL: https://www.iso.org/standard/54534.html

6. (2013) ISO/IEC 27002: Information Technology — Security Techniques — Code of Practice for Information Security Controls. URL: https://www.iso.org/standard/54533.html

7. 2020 ISO Survey of Management System Standards reveals 17% increase in certifications. URL: https://www.quality.org/article/2020-iso-survey-management-system-standards-reveals-17- increase-certifications

8. MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. URL: https://msecb.com/wp-content/uploads/2023/01/MSECB-Transition-Policy-on-MS-Certification-to-ISOIEC27001.pdf?utm_source=sendinblue&utm_campaign=Clients%20ISOIEC%20270012022%20Transition% 20Policy&utm_medium=email

9. Global Cybersecurity Outlook 2022. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2022

10. ISO/IEC 27001: What's new in IT security? URL: https://www.iso.org/contents/news/2022/10/new-iso-iec27001.html

11. What Are The ISO 27001 Changes In 2022. URL: https://bestpractice.biz/what-are-the-iso-27001-changes-in2022/

12. ISO 27001 2013 vs. 2022 revision – What has changed? URL: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/

13. ISO/IEC 27001 - What are the main changes in 2022? URL: https://pecb.com/article/isoiec-27001---what-arethe-main-changes-in-2022

14. ISO 27001: Аналіз змін та особливості відповідності новій версії стандарту. URL: file:///C:/Users/user/Downloads/Admin,+004.pdf

15. IT-безпека та інформаційна безпека – у чому різниця? URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/it-bezpeka-ta-informacijna-bezpeka-%E2%80%93-u-chomu-riznicya

Електронні ресурси

1. International Communications Consultancy Organisation URL: http://www.iccopr.com

2. Законодавство України. URL: http://zakon4.rada.gov.ua/laws
3. Інтернет-портал для управлінців. URL: www. Management.com.ua
4. Портал управління змінами. URL: https://pdp.nacs.gov.ua/
5. Психологічний захист та його механізм. URL: www.horting.org.ua/note/1455
6. Сайт наукової бібліотеки «Буковина». URL: http://buklib.net
7. Сайт Національної бібліотеки імені В.І. Вернадського. URL: http://www.nbuv.gov.ua/
8. Українські підручники он-лайн. URL: http://pidruchniki.ws
9. International Security and Partnership Center, Центр міжнародної безпеки та партнерства. URL: www.ispc.org.ua

Розглянуто і схвалено на засіданні кафедри ЕМтаКД, Протокол №1 від «28» серпня 2024 р.