Силабус
навчальної дисципліни
Кібербезпека в цифровому середовищі
2024-2025 навчальний рік

Освітня програма «Цифрові технології»
Спеціальність 015 Професійна освіта (Цифрові технології)
Освітня програма «Середня освіта. Інформатика»
Спеціальність 014 Середня освіта (Інформатика)
Галузь знань 01 Освіта/Педагогіка
Рівень вищої освіти перший

Викладач	Антоненко Олександр Володимирович
Посилання на сайт	
Контактний тел.	
E-mail викладача:	oleksandrantonenkobdpu@gmail.com
Графік консультацій	Вівторок 13:00-14:15

Обсяг курсу на поточний навчальний рік:

Денне

Кількість кредитів/ годин	Лекції	Лабораторні заняття	Самостійна робота	звітність
5/150	26	24	110	залік

Заочне

Кількість кредитів/ годин	Лекції	Лабораторні заняття	Самостійна робота	звітність
5/150	8	10	132	залік

Семестр: осінній/~~весняний~~
Мова навчання: українська
Ключові слова: інформаційна безпека, захист інформації, політики безпеки, служби безпеки.
Мета та предмет курсу: сформувати та розвинути у здобувачів курсу професійні компетенції, що дозволяють їм застосовувати сучасні технології захисту інформації, вибирати засоби та інструменти захисту інформації, які мінімізують загрози несанкціонованого доступу до даних. Формування у здобувачів знань, умінь, навичок та досвіду діяльності, які характеризують етапи формування компетенцій у галузі цифрової

економіки та розвитку цифрової грамотності учасників освітнього процесу, освоєнні професійної компетенції у сфері інформаційної безпеки (кібербезпеки)..

Компетентності та програмні результати навчання:

Загальні компетентності:

- ЗК Здатність знаходити, обробляти, інформацію з різних джерел, аналізувати та синтезувати на основі перевірених фактів та логічних аргументів.
- ЗК Здатність приймати обґрунтовані рішення.
- ЗК Навички використання інформаційних і комунікаційних технологій.

Фахові компетентності:

- ФК Здатність до використання методик навчання учнів загальноосвітньої школи інформаційно-комунікаційним технологіям.
- ФК Здатність до обліку та аналізу управління процесом навчання учнів загальноосвітньої школи інформаційно-комунікаційним технологіям.
- СК Здатність управляти комплексними діями / проектами, відповідати за прийняття рішень у непередбачуваних умовах та професійний розвиток здобувачів освіти і підлеглих
- СК Здатність аналізувати ефективність проектних рішень, пов'язаних з підбором, експлуатацією, удосконаленням, модернізацією технологічного обладнання та устаткування галузі/сфери відповідно до спеціалізації.

Результати навчання:

- ПР Створювати інструкції, паспорти комп'ютерних класів з вимогами до безпечного отримання, оброблення та передавання інформації..
- ПР Встановлювати та налаштовувати програмні засоби захисту інформації.
- ПР Ідентифікувати загрози й обирати відповідні дії для знешкодження цих загроз.
- ПР Виявляти підозрілу активність в системі та знешкоджувати її
- ПР Аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення
- ПР Застосовувати міжнародні та національні стандарти і практики в професійній діяльності

Зміст курсу:

Змістовий модуль 1. Вступ до кіберзахисту.

Основні поняття та термінології. Значення кібербезпеки для національного захисту та індивідуальної приватності.

Тема 1 Вступ до кіберзахисту.

Основні поняття та терміни: «кібератака», «вразливість», «шкідливе програмне забезпечення (малвар)», «фішинг», «рансомваре», та інші. Основи криптографії, принципи безпечної інтернет-поведінки.

Тема 2 Значення кібербезпеки для національного захисту.

Захист національної інфраструктури та урядових установ, забезпечення приватності та безпеки індивідуальних користувачів інтернету. Вплив кібербезпеки на економіку, політику та соціальне життя.

Тема 3 Кібератаки і їх вплив на державні установи

Аналіз атак типу WannaCry, NotPetya та інші. Використання вразливостей в програмному забезпеченні та інфраструктурі проти організацій та цілих країн, висновки з інцидентів для покращення власної кібербезпеки.

Змістовий модуль 2. Загрози та вразливості.

Основні види кіберзагроз. Методи розпізнавання та запобігання кібератакам. Актуальні схеми шахрайства та соціальної інженерії.

Тема 1. Основні види кіберзагроз.

Фішинг, віруси та троянські програми, ransomware, спам та інші.

Тема 2. Методи розпізнавання та запобігання кібератакам.

Розпізнавання фішингових атак, підозрілих файлів, листів. Організація технічних заходів з кібербезпеки та зменшення ризиків: робота з даними, багатофакторна аутентифікація; мінімізація привілеїв доступу до інформації. Виявлення та реагування на інциденти (рекомендований план дій у випадку інцидентів пов'язаних з кібербезпекою). Конфіденційність у інтернеті, зокрема у соціальних мережах

Тема 3. Поняття соціальної інженерії та приклади актуальних схем шахрайства.

Базове поняття: соціальна інженерія, інженерія соціальних мереж.

Змістовий модуль 3 Кібербезпека учасників освітнього процесу

Тема 1. Он-лайн та оф-лайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу

Конфіденційність, цілісність та доступність даних. Наслідки порушення безпеки. Он-лайн та оф-лайн ідентифікація. Приватні дані та місця їх розташування. Причини викрадення даних. Бездротові з'єднання, автентифікація та стійкі паролі. Методи та засоби захисту конфіденційної інформації при використанні Інтернету. Типи порушників у сфері кібербезпеки. Внутрішні та зовнішні загрози. Правові проблеми кібербезпеки. Захист організації.

Тема 2. Забезпечення інформаційної безпеки учасників освітнього процесу

Інформаційна безпека здобувачів освіти. Документи, що регламентують роботу закладу освіти з персональними даними, плани заходів щодо забезпечення інформаційної безпеки здобувачів освіти. Кібербезпека учасників освітнього процесу.

Тема 3. Удосконалення рівня цифрової компетентності учасників освітнього процесу з кібербезпеки: інструменти, технології

Сучасні міжнародні програми у галузі кібербезпеки, напрями подальшого підвищення кваліфікації. Знайомство із середовищем дистанційної освіти Cisco NetAcad міжнародної мережевої академії Cisco та CRDF Global

Методи навчання:

- методи організації і здійснення навчально-пізнавальної діяльності:
  - пояснення;
  - розповідь;
  - бесіда;
  - ілюстрування;
  - демонстрування;
  - самостійне спостереження;
  - практичні і дослідні роботи;
- методи стимулювання навчальної діяльності:
  - створення ситуації інтересу у процесі викладення;
  - створення ситуації новизни;
  - опора на життєвий досвід студента;
  - стимулювання обов'язку і відповідальності в навчанні;
- методи контролю і самоконтролю у навчанні:
  - індивідуальне опитування, фронтальне опитування, комбіноване опитування;
  - тестовий, самоконтроль і самооцінка.

Політика курсу (особливості проведення навчальних занять): очне, заочне, дистанційне, робота з лабораторним обладнанням.

Політика освітньої компоненти ґрунтується на засадах академічної доброчесності, прийнятої в Університеті *(https://bdpu.org.ua/wp-content/uploads/2020/03/akademdobrochesnist-*

_sayt.pdf). Не допускається академічний плагіат, фальсифікація і фабрикація даних, списування; забороняється використання здобувачами освіти додаткових джерел інформації під час оцінювання навчальних результатів (у тому числі засобами електронного зв'язку). Якщо у ході освітньої діяльності здобувач використовує інтернет-ресурси, штучний інтелект або інші джерела інформації, він має про це обов'язково вказувати (наводити відповідні посилання).

Технічне й програмне забезпечення/обладнання, наочність: лабораторне обладнання, спеціалізоване програмне забезпечення.

Система оцінювання та вимоги:

1. Поточний контроль
- звіт з лабораторної роботи;
- звіт з самостійної роботи;
- індивідуальне завдання;
- індивідуальне опитування;
- фронтальне опитування;
- комбіноване опитування;

2. Залік

Оцінка за університетською шкалою	*Оцінка за шкалою ECTS*
90 – 100	A
78 – 89	B
65 – 77	C
58 – 64	D
50 – 57	E
35 – 49	FX (з можливістю повторного складання)
1 – 34	F (з обов'язковим повторним вивченням ОК)

Критерії оцінювання завдань змістових модулів

Максимальна кількість балів разом із самостійною роботою за кожну тему становить 25 балів. Система нарахування балів подана в таблиці. Контроль включає оцінювання знань, умінь та навичок.

Завдання оцінюється 10-ма балами, якщо відповідь правильна, повна, з достатнім теоретичним обґрунтуванням, позначена елементами творчості; має місце аргументація особистої позиції, правильно оформлена лабораторна робота.

Оцінка "8-9 бали": відповідь правильна, логічна, обґрунтована, але без елементів власних суджень, правильно оформлена лабораторна робота..

Оцінка "6-7 бали": в цілому завдання виконано правильно, повністю, проте мають місце окремі неточності, або розв'язання не містить належного теоретичного обґрунтування, правильно оформлена лабораторна робота..

Оцінка "4-5 бали": відповідь неповна, поверхова, характеризується відсутністю самостійного аналізу, правильно оформлена лабораторна робота..

Оцінка "2-3 бал": відповідь елементарна, фрагментарна, що зумовлено нечітким уявленням про предмет питання, правильно оформлена лабораторна робота..

Оцінка "1 бал": тільки правильно оформлена лабораторна робота.

Оцінка "0 балів": неправильна відповідь або її відсутність, лабораторна робота не оформлена.

Система рейтингових (вагових) балів та критерії оцінювання

Лабораторні роботи. Ваговий бал – 10, в тому числі підготовка протоколу – 2 бали, виконання роботи – 4 бали, захист роботи – 4 бали.

*0..2 підготовка протоколу :*2 – якісна підготовка, акуратно оформлений протокол лабораторної роботи; 1 - наявність недоліків у оформленні протоколу лабораторної роботи; 0 – грубі помилки при оформленні протоколу лабораторної роботи, протокол відсутній

0..4 виконання роботи, захист роботи: 4 – акуратне та правильне виконання роботи, логічна та послідовна відповідь при захисті лабораторної роботи; 3 – наявність незначних недоліків у відповідях при виконанні, захисті лабораторної роботи; 2-1 – наявність недоліків у виконанні, у відповідях при захисті лабораторної роботи, протоколі; 0 –відсутність виконання роботи, грубі помилки при інтерпретації результатів розрахунку, студент неспроможний захистити роботу.

Штрафні бали.

Несвоєчасний захист лабораторної роботи, незадовільний вхідний контроль – (1..5) балів

Заохочувальні бали.

Участь у модернізації лабораторних робіт, удосконаленні дидактичних матеріалів 5..15 балів Інформаційний пошук та підготовка реферату з наданої викладачем теми 5..10 балів

Список рекомендованих джерел

Основні

1. 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.
2. Про захист персональних даних: за станом на 19.08.2022 / Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс].— Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Про національну безпеку України: : за станом на 15.06.2022 р. / Закон України, затверджений ВР України 21.06.2018 р., № 2469-VIII [Електронний ресурс].— Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text
4. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518. URL: https://cutt.ly/tw0Hilwp.
5. Про Національну програму інформатизації: за станом на 01.01.2022 / Закон України від 04.02.1998 р. № 74/98-ВР [Електронний ресурс].— Режим доступу: http://zakon0.rada.gov.ua/laws/show/74/98-вр
6. Про основні засади забезпечення кібербезпеки України: За станом на 17.08.2022 / Закон України, затверджений ВР України 05.10.2017 р. № 2163-VIII [Електронний ресурс].— Режим доступу: http://zakon0.rada.gov.ua/laws/show/2163-19
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://cutt.ly/ew0HtIOO.
8. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

Додаткові

9. Антоненко О.В. Криптографічні методи перетворення інформації / О.В. Антоненко - Навчальний посібник + CD для студентів вищих педагогічних навчальних закладів напряму підготовки 6.010104 Професійна освіта (Комп'ютерні технології). – Бердянськ, 2015. – 177 с.
10. Бабак, В.П. Інформаційна безпека та сучасні мережеві технології: Англо-Українсько-Російський словник термінів. / В.П. Бабак, О.Г. Корченко. — К.:НАУ, 2003. — 670 с.: іл.

11. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу / НД ТЗІ 2.5-010-03. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2003. 24 с. URL: https://cutt.ly/2w0HvZip.

12. Захист дітей у цифровому середовищі: рекомендації для батьків та освітян, 2020. Режим доступу: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines-for-Parents-Educators-UAfin.pdf

13. Ігнатушко Ю.І. Правові засади регулювання забезпечення кібербезпеки в Україні VIII [Електронний ресурс].— Режим доступу: http://dspace.oduvs.edu.ua/bitstream/123456789/471/1/ilovepdf_com-18-19%5B1%5D.pdf

14. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації.— 2013.— Т. 19, № 1.— с. 40–45

15. Курс мережевої академії Cisco: Cybersecurity Essentials, 2020. Режим доступу: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

16. Митник К., Вемосі Р. Мистецтво залишатися непоміченим. Хто ще читає ваші імейли? / пер. з англ. О. Асташової. Київ : Наш формат, 2019. 278 с.

17. Мукоіда Р., Аносєнков А. Правове забезпечення захисту персональних даних в Україні. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.-практ. конф., 26 листопада 2020 р. Одеса : ОДУВС, 2021. С. 3-8.

18. Нашинець -Наумова, А. Інформаційна безпека як складова частина національної безпеки України. / А Нашинець -Наумова // Підприємництво, господарство і право. — 2013. — №8. – С.63–66.

19. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів / Information systems and networks. 2022. Вип. 12. С. 7-16.

20. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с

21. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу/ НД ТЗІ 3.6-001-2000. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000. 8 с. URL: https://cutt.ly/qw0HhdQT.