Силабус
навчальної дисципліни
Захист інформації
2025-2026 навчальний рік

Освітня програма «Середня освіта (Інформатика)»
Спеціальність 014 Середня освіта
Предметна спеціальність 014.09 Середня освіта (Інформатика)
Галузь знань 01 Освіта/Педагогіка
Рівень вищої освіти перший

Викладач	Антоненко Олександр Володимирович
Посилання на сайт	https://bdpu.org.ua/teachers/antonenko-oleksandr-volodymyrovych/
Контактний тел.	+38(073)738-74-84
E-mail викладача:	oleksandrantonenkobdpu@gmail.com
Графік консультацій	Понеділок 13:00-14:00

Обсяг курсу на поточний навчальний рік:

Денне

Кількість кредитів/ годин	Лекції	Практичні заняття	Самостійна робота	звітність
3/90	26	24	100	екзамен

Заочне

Кількість кредитів/ годин	Лекції	Практичні заняття	Самостійна робота	звітність
3/90	10	10	130	екзамен

Семестр: осінній/~~весняний~~
Мова навчання: українська
Ключові слова: інформаційна безпека, захист інформації, політики безпеки, служби безпеки.
Мета та предмет курсу: метою викладання навчальної дисципліни "Захист інформації" є надання здобувачам вищої освіти знань з комплексу проблем інформаційної безпеки, побудови, функціонування й удосконалювання правових, організаційних, технічних і технологічних процесів, що забезпечують інформаційну безпеку й формують структуру системи захисту коштовної й конфіденційної інформації.

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.

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.

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

Зміст курсу:

Змістовий модуль 1.

Тема 1. Визначення інформаційної безпеки

Тема 2. Категорії атак

Змістовий модуль 2.

Тема 3. Методи хакерів

Тема 4. Служби інформаційної безпеки

Змістовий модуль 3.

Тема 5. Політика безпеки

Тема 6. Керування ризиком

Змістовий модуль 4.

Тема 7. Забезпечення інформаційної безпеки

Тема 8. Електронна комерція: вимоги безпеки

Змістовий модуль 5.

Тема 9. Перехоплення інформації за допомогою електронних засобів. Техніка перехоплення телефонних розмов

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: спеціалізоване програмне забезпечення.

Система оцінювання та вимоги:

1. Поточний контроль

- звіт з практичної роботи;
- звіт з самостійної роботи;
- індивідуальне завдання;
- індивідуальне опитування;
- фронтальне опитування;
- комбіноване опитування;

2. Екзамен

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 практична робота.

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

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

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

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

Оцінка "0 балів": неправильна відповідь або її відсутність, практична робота не

оформлена.

Система рейтингових (вагових) балів та критерії оцінювання

Практичні 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 практичної роботи, протокол відсутній

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

Штрафні бали.

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

Заохочувальні бали.

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

Список рекомендованих джерел

Базова

1. Білик М. А. Системи захисту інформації: теорія та практика . – Київ: АБВ, 2020. – 230 с.
2. Білоус О. П. Захист інформаційних ресурсів в інформаційних системах . – Львів: Видавництво ЛНУ, 2020. – 299 с.
3. Бондаренко О. І., Горбаченко В. Г. Основи захисту інформаційних систем . – Харків: ХНУРЕ, 2018. – 254 с.
4. Боярчук А. В. Захист інформаційних ресурсів в кіберпросторі . – Харків: НТУ "ХПІ", 2018. – 268 с.
5. Воробйов Ю. В. Організація систем захисту інформаційних ресурсів . – Одеса: ОНУ, 2017. – 256 с.
6. Горбенко О. Г. Інформаційна безпека та управління ризиками . – Київ: Вид. центр НАУ, 2019. – 210 с.
7. Дорошенко В. Г. Інформаційна безпека: принципи та засоби . – Київ: ВНТУ, 2021. – 322 с.
8. Дячук І. В. Захист даних в інформаційних системах . – Одеса: ОНУ, 2020. – 210 с.
9. Коваленко Ю. В., Лазоренко М. В. Інформаційна безпека та криптографія . – Харків: Фоліо, 2017. – 204 с.
10. Коваль М. В. Захист інформації у комп'ютерних системах . – Київ: Політехніка, 2021. – 284 с.
11. Ковальчук А. В. Основи безпеки інформаційних ресурсів . – Харків: Основа, 2016. – 278 с.
12. Кузьменко А. С. Методологія забезпечення інформаційної безпеки . – Харків: ХНУ, 2018. – 299 с.
13. Лисенко І. А. Методи захисту інформаційних ресурсів в інформаційно-комунікаційних системах . – Львів: ЛНУ, 2020. – 198 с.
14. Литвиненко А. І. Організація інформаційної безпеки в комп'ютерних мережах . – Харків: Фоліо, 2020. – 264 с.

15. Мартиненко О. С. Основи безпеки інформаційних технологій . – Одеса: ОНУ, 2019. – 244 с.

16. Мельник В. Г. Теоретичні основи захисту інформаційних ресурсів . – Київ: Вид. центр КНУ, 2019. – 312 с.

17. Паращенко С. А. Захист інформації в комп'ютерних мережах . – Київ: НТУУ КПІ, 2018. – 215 с.

18. Поліщук С. А. Кібербезпека: Основи захисту інформації . – Вінниця: ВНТУ, 2021. – 320 с.

19. Руденко О. М. Методи та засоби захисту інформаційних ресурсів . – Харків: Видавництво ХНУ, 2016. – 236 с.

20. Семенов М. В. Методи захисту інформаційних ресурсів в мережах . – Харків: ХНУ, 2018. – 232 с.

21. Тимофєєв О. Г. Кібербезпека: основи і практики . – Львів: ЛНУ, 2017. – 318 с.

22. Ткачук В. О. Захист інформації в кіберпросторі . – Київ: Політехніка, 2021. – 278 с.

23. Чернявський М. А. Інформаційна безпека і конфіденційність . – Київ: Техніка, 2019. – 262 с.

24. Чорний С. П. Кіберзахист та інформаційна безпека . – Київ: АВД, 2020. – 284 с.

25. Шаров Ю. А. Основи криптографії та захисту інформації . – Київ: Освіта України, 2016. – 276 с.

26. Яцишина О. П. Сучасні методи захисту інформаційних ресурсів . – Львів: Видавництво ЛНУ, 2019. – 218 с.

Допоміжна

1. 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.

2. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань : [б.в.], 2012.-120 с.

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