

Приватний вищий навчальний заклад «Буковинський університет»
(повне найменування вищого навчального закладу)

Факультет інформаційних технологій та економіки
(назва інституту / факультету)

Кафедра комп'ютерних систем і технологій
(назва кафедри)

ЗАТВЕРДЖУЮ»
Декан факультету
інформаційних технологій та економіки
Штерма Т.В.
«28» 2021 р.

СИЛАБУС
навчальної дисципліни

Технології захисту інформації

обов'язкова навчальна дисципліна
(вказати: обов'язкова / вибіркова)

Освітньо-професійна програма «КОМП'ЮТЕРНІ НАУКИ»
(назва програми)

Спеціальність 122 «Комп'ютерні науки»
(вказати: код, назва)

Галузь знань 12 «Інформаційні технології»
(вказати: шифр, назва)

Рівень вищої освіти перший бакалаврський
(вказати: перший бакалаврський/другий магістерський)

Факультет _____
(назва факультету, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання українська
(вказати: на якій мові читається дисципліна)

Розробник: Артеменко О.І., завідувач кафедри комп'ютерних систем і технологій, к.т.н., доцент
(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Профайл викладача (-ів) _____
(посилання на сторінку кафедри з інформацією про викладача (-ів))

Контактний тел.

E-mail: olha.i.artemenko@lpnu.ua

Посилання на сторінку курсу на сайті дистанційного навчання університету

Консультації четвер з 10.00 до 16.00.

1. Анотація дисципліни (призначення навчальної дисципліни).

Предметом навчальної дисципліни є:

- алгоритмічне забезпечення засобів захисту інформації;
- програмне забезпечення засобів захисту інформації;
- методики побудови захисту інформації в інформаційних системах;
- сучасні засоби взаємодії людини з апаратним і програмним забезпеченням.

Після вивчення дисципліни студенти повинні:

Знати:

- теоретичні основи крипто захисту даних;
- предмет, методи та завдання захисту даних;
- методики захисту важливої інформації від несанкціонованого доступу;
- механізм шифрування інформації з допомогою існуючих методів шифрування;
- основні методи математичного перетворення інформації та способи її відтворення;
- загальні принципи захисту мереж і баз даних;
- основні напрямки використання криптографічних методів;
- принципи застосування положень теорії захисту інформації в сучасних електронно-обчислювальних системах та мережах.

Вміти:

- застосовувати математичний апарат теорії захисту інформації для вирішення практичних задач;
 - використовувати методи оптимального захисту мереж та баз даних для побудови безпечних інформаційних систем;
 - виконувати вибір та застосовувати методи шифрування/дешифрування для забезпечення достовірності передачі повідомлень;
- розробляти схеми систем безпечної передачі інформації по незахищених каналах зв'язку.

2. Мета та завдання навчальної дисципліни:

Мета викладання дисципліни: підготувати майбутніх фахівців до ефективного використання сучасних інформаційних технологій в процесі розв'язування завдань безпеки даних та захисту цифрової інформації.

Завдання: засвоєння знань, умінь і навичок з основ захисту інформації і набуття навичок практичного їх застосування при роботі з сучасним прикладним програмним забезпеченням.

3. Пререквізити.

Теорія алгоритмів,
Об'єктно-орієнтоване програмування,
Інформатика та комп'ютерна техніка

4. Компетентності та результати навчання, формуванню яких сприяє дисципліна (взаємозв'язок з нормативним змістом підготовки здобувачів вищої освіти, сформульованим у термінах результатів навчання):

Під час вивчення дисципліни, відповідно до освітньо-професійної програми, формуються наступні:

Інтегральна компетентність

Бакалавр здатний вирішувати спеціалізовані задачі та практичні проблеми в області комп'ютерних наук при здійсненні професійної діяльності або в процесі навчання.

Загальні компетентності (ЗК)

- ЗК2. Здатність працювати в команді та особисто. Навички міжособистісної взаємодії
ЗК3. Здатність вчитися і оволодівати сучасними знаннями
ЗК4. Навички здійснення безпечної діяльності
ЗК7. Навички використання інформаційних і комунікаційних технологій
ЗК8. Здатність застосовувати знання у практичних ситуаціях

Фахові компетентності спеціальності (ФК)

- ФК6. Здатність використовувати сучасні технології проектування в розробці алгоритмічного та програмного забезпечення комп'ютерних систем і технологій
ФК7. Здатність застосовувати, впроваджувати та експлуатувати сучасні комп'ютерних систем і технологій (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних, бізнес-аналітики) у різних галузях людської діяльності, національної економіки та виробництва
ФК11. Вибирати, проектувати, розгортати, інтегрувати, управляти, адмініструвати та супроводжувати застосування комунікаційних мереж, сервісів та інфраструктури організації
ФК12. Здатність здійснювати організацію робочих місць, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів організаційно-управлінської діяльності

Отримуються наступні програмні результати навчання:

- ПРН34. Знати, розуміти і застосовувати сучасні підходи щодо оцінки та забезпечення якості програмного забезпечення.
ПРН35. Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.
ПРН36. Знати, розуміти, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.
ПРН38. Вміння використовувати інформаційні та комунікативні технології при спілкуванні, обміні, зборі, аналізі, обробці інформації.

5. Опис навчальної дисципліни

5.1. Загальна інформація

| Найменування показників | Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень | Характеристика навчальної дисципліни | |
|---|--|--------------------------------------|-----------------------|
| | | денна форма навчання | заочна форма навчання |
| Кількість кредитів – 4 | Галузь знань 12 «Інформаційні технології» | Нормативна | |
| Модулів – 2 | Спеціальність: 122 «Комп'ютерні науки» | Рік підготовки: | |
| Загальна кількість годин - 135 | | 4-й | -й |
| | | Семестр | |
| | | 7-й | -й |
| Тижневих годин для денної форми навчання: | Освітній-ступінь:бакалавр | Лекції | |
| | | 18 год. | год. |
| | | Практичні, семінарські | |

| | | |
|--|-------------------------------------|------|
| аудиторних – 3 самостійної роботи студента - 6 | 20 год. | год. |
| | Лабораторні | |
| | 10 год. | год. |
| | Самостійна робота | |
| | 87 год. | год. |
| | Індивідуальні завдання: год. | |
| Вид контролю: екзамен | | |

5.2. Структура навчальної дисципліни

| № теми | Назва теми | Кількість годин | | | |
|---|--|-----------------|-----------|-------------|-----------|
| | | Лекції | Практичні | Лабораторні | СРС |
| МОДУЛЬ 1 | | | | | |
| 1. | Сучасні аспекти інформаційної безпеки | 2 | | | 14 |
| 2. | Порушення, механізми і служби захисту | 2 | | | |
| 3. | Побудова резервних копій баз даних | | | 2 | |
| 4. | Хакінг архівних даних | | 2 | | |
| 5. | Історія розвитку систем шифрування. Основні терміни та вимоги до криптосистем | 2 | | | 14 |
| 6. | Симетричні криптосистеми | | | | 14 |
| 7. | Алгоритми традиційного шифрування | 2 | | | |
| 8. | Шифр Цезаря | | 2 | | |
| 9. | Шифри заміни | | 2 | | |
| 10. | Шифр Віжинера | | 2 | | |
| 11. | Біграмні шифри | | | 2 | |
| 12. | Алгоритми криптографії з відкритим ключем | 2 | | | |
| 13. | Створення цифрового підпису | | | 2 | |
| 14. | Модульна контрольна робота №1 | | 2 | | |
| Всього по модулю 1 (годин) | | 10 | 10 | 6 | 42 |
| <i>Всього по модулю (поточний контроль в балах)</i> | | 5 | 8 | 6 | 6 |
| <i>Модульна контрольна робота №1 (бали)</i> | | 10 | | | |
| Всього по модулю 1 (балів) | | 35 балів | | | |
| МОДУЛЬ 2 | | | | | |
| 15. | Методи аутентифікації повідомлень | | | | 15 |
| 16. | Виявлення вторгнень | 2 | | | 15 |
| 17. | Захист електронної пошти і шифрування файлів | | 2 | | |
| 18. | Криптоаналіз симетричних систем | | 4 | | |
| 19. | Електронний цифровий підпис | 2 | | | |
| 20. | Адміністрування та моніторинг локальної мережі | | | 2 | |

| | | | | | |
|---|--------------------------------|------------------|-----------|-----------|-----------|
| 21. | Встановлення мережевого екрану | 2 | | | 15 |
| 22. | Стеганографія | | | 2 | |
| 23. | Створення VPN-мережі | 2 | | | |
| 24. | Сканування мережі | | 2 | | |
| 25. | Модульна контрольна робота №2 | | 2 | | |
| Всього по модулю 2 (годин) | | 8 | 10 | 4 | 45 |
| Всього по модулю (поточний контроль в балах) | | 4 | 9 | 6 | 6 |
| Модульна контрольна робота №2 (бали) | | 10 | | | |
| Всього по модулю 2 (балів) | | 35 балів | | | |
| Екзамен (бали) | | 30 | | | |
| РАЗОМ (годин) | | 18 | 20 | 10 | 87 |
| РАЗОМ (балів) | | 100 балів | | | |

5.3. Теми лабораторних занять

| № лабораторного заняття | Назва лабораторної роботи | Кількість годин |
|--|--|-----------------|
| з/п | | |
| МОДУЛЬ 1 | | |
| 1. | Побудова резервних копій баз даних | 2 |
| 2. | Створення цифрового підпису | 4 |
| Всього по модулю (годин) | | 6 |
| МОДУЛЬ 2 | | |
| 3. | Адміністрування та моніторинг локальної мережі | 2 |
| 4. | Стеганографія | 2 |
| Всього по модулю (годин) | | 4 |
| РАЗОМ ЗА СЕМЕСТР ЛАБОРАТОРНИХ (годин) | | 10 |

5.4. Зміст завдань для самостійної роботи

| № СРС з/п | Назва самостійної роботи студента | Кількість годин |
|-----------------|---------------------------------------|-----------------|
| МОДУЛЬ 1 | | |
| 1. | Сучасні аспекти інформаційної безпеки | 14 |
| 2. | Історія розвитку систем шифрування | 14 |

| | | |
|---|-----------------------------------|-----------|
| 3. | Симетричні криптосистеми | 14 |
| Всього по модулю (годин) | | 42 |
| МОДУЛЬ 2 | | |
| 4. | Методи аутентифікації повідомлень | 15 |
| 5. | Виявлення вторгнень | 15 |
| 6. | Встановлення мережевого екрану | 15 |
| Всього по модулю (годин) | | 45 |
| РАЗОМ ЗА СЕМЕСТР САМОСТІЙНИХ (годин) | | 87 |

6. Система контролю та оцінювання

Об'єктом поточного контролю знань студентів є:

- систематичність, якість та своєчасність виконання і захисту практичних робіт;
- систематичність, якість та своєчасність виконання і захисту лабораторних робіт;
- систематичність та своєчасність виконання завдань самостійної роботи студента;
- якість виконання модульних контрольних робіт.

Дисципліна «Технології захисту інформації» складається з двох модулів, оцінювання яких здійснюється за результатами 6 практичних робіт та 4 лабораторних робіт, двох модульних контрольних робіт та самостійної роботи студента.

Перевірка виконання завдань самостійної роботи студента виконується на передостанньому занятті кожного модуля. Кожне завдання самостійної роботи студента оцінюється в 2 бала.

Предметом оцінювання на модульних контрольних роботах є вузлові питання програми та типові задачі, що потребують творчої відповіді та уміння синтезувати отримані знання і застосувати їх при вирішенні практичних задач. Контрольні роботи виконуються письмово, кожна з них оцінюється в 10 балів. Перелік та зміст модульних завдань включено до робочої програми дисципліни.

Підсумковий контроль знань проводиться у формі іспиту.

Об'єктом оцінювання є результати письмової відповіді студента на теоретичні запитання екзаменаційного білета, а також виконання практичних задач. На іспит виносяться вузлові питання програми та типові задачі, що потребують творчої відповіді та уміння синтезувати отримані знання і застосувати їх при вирішенні практичних задач. Максимально можлива оцінка за іспит 30 балів.

Критерії оцінювання результатів навчання з навчальної дисципліни

Виконання практичних робіт оцінюється за результатами своєчасного захисту відповідних звітів. Звіт з практичної роботи повинен бути зданий викладачу впродовж двох наступних пар з дисципліни. Звіт з останньої практичної роботи здається перед початком модульної контрольної роботи №2. За прострочення терміну здачі звіту з практичної роботи віднімаються бали від максимальної вартості практичної роботи: кожен тиждень прострочення віднімає 1 бал від можливої оцінки за дану роботу. Звіт з практичної роботи має містити титульний аркуш за встановленою формою і результати виконання всіх завдань роботи. До захисту приймаються тільки звіти, підготовлені і роздруковані з допомогою текстового редактора Microsoft Word.

Максимально можливі оцінки за практичні роботи 3 бали.

Кожна практична робота оцінюється за такою шкалою:

- подані результати є правильними, звіт повністю відповідає вимогам, грамотно і акуратно оформлений, відповіді на поставлені в завданнях питання є повними і точними – **3 бали**;
- звіт містить незначні похибки у виконанні завдань, грамотно і акуратно оформлений з виконанням всіх вимог – **1-2 бали**;
- звіт не відповідає вимогам, містить результати виконання чужого індивідуального завдання; студент здає звіт значно пізніше встановленого викладачем терміну – **0 балів**.

Виконання лабораторних робіт оцінюється за результатами своєчасного захисту відповідних звітів. Звіт з лабораторної роботи повинен бути зданий викладачу впродовж двох наступних пар з дисципліни. Звіт з останньої лабораторної роботи здається перед початком модульної контрольної роботи №2. За прострочення терміну здачі звіту з лабораторної роботи віднімаються бали від максимальної вартості лабораторної роботи: кожен тиждень прострочення віднімає 1 бал від можливої оцінки за дану роботу. Звіт з лабораторної роботи має містити титульний аркуш за встановленою формою і результати виконання всіх завдань роботи. До захисту приймаються тільки звіти, підготовлені і роздруковані з допомогою текстового редактора Microsoft Word.

Максимально можливі оцінки за лабораторні роботи 3 бали.

Кожна лабораторна робота оцінюється за такою шкалою:

- подані результати є правильними, звіт повністю відповідає вимогам, грамотно і акуратно оформлений, відповіді на поставлені в завданнях питання є повними і точними – **3 бали**;
- звіт містить незначні похибки у виконанні завдань, грамотно і акуратно оформлений з виконанням всіх вимог – **1-2 бали**;
- звіт не відповідає вимогам, містить результати виконання чужого індивідуального завдання; студент здає звіт значно пізніше встановленого викладачем терміну – **0 балів**.

Шкала оцінювання: національна та ЄКТС

| СУМА БАЛІВ | ОЦІНКА ЄКТС | ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ | |
|------------|-------------|-------------------------------|--------------|
| | | екзамен | залік |
| 90-100 | A | відмінно | відмінно |
| 82-89 | B | добре | добре |
| 74-81 | C | | |
| 64-73 | D | задовільно | задовільно |
| 60-63 | E | | |
| 35-59 | FX | незадовільно | незадовільно |
| 1-34 | F | | |

Розподіл балів з навчальної дисципліни Розподіл балів, які отримують студенти

| № теми | Модуль | Кількість годин | | | |
|---|--------|-----------------|-----------|-------------|----------|
| | | Лекції | Практичні | Лабораторні | СРС |
| МОДУЛЬ 1 | | | | | |
| Всього по модулю (поточний контроль в балах) | | 5 | 8 | 6 | 6 |

| | | | | |
|---|------------------|----------|----------|----------|
| Модульна контрольна робота №1 (бали) | 10 | | | |
| Всього по модулю 1 (балів) | 35 балів | | | |
| МОДУЛЬ 2 | | | | |
| Всього по модулю (поточний контроль в балах) | 4 | 9 | 6 | 6 |
| Модульна контрольна робота №2 (бали) | 10 | | | |
| Всього по модулю 2 (балів) | 35 балів | | | |
| Екзамен (бали) | 30 | | | |
| РАЗОМ (балів) | 100 балів | | | |

7. Рекомендована література

Основна:

1. Технології захисту інформації : навч. посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.
2. Жураковский Ю.П., Полторац В.П. Теорія інформації кодування: Підручник. - Київ : Вища школа, 2001. - 255 с.
3. Теорія інформації та кодування : навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Дніпродзержинськ : Національний гірничий університет, 2012. – 108 с.
4. Захист інформації в автоматизованих системах управління : навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
5. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. / В.Е. Козлов. – Горячая линия – Телеком, 2002. – 336 с.
6. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – Київ: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с..
7. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – Київ: Арий, 2008. – Том II. Информационная безопасность. – 344 с.

Допоміжна:

1. Літнарівч Р.М. Сучасні технології інформаційної безпеки. Част. 1. Навчальний посібник. – МЕНУ, Рівне, 2011. – 97 с.
2. В.А. Хорошко. Методы и средства защиты информации. / В.А. Хорошко, А.А. Чекотков. – К.: Юніор, 2003. - 479 с.
3. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2005. - 688 с.
4. Цымбал В.П. Задачник по теории информации и кодирования. - Киев: Издательское объединение “Вища школа”, 2000. – 268 с.
5. Лигун А.О., Комп’ютерна графіка (Обробка та стиск зображень) / А.О.Лигун, О.О.Шумейко . – Дніпропетровськ: Біла К.О., 2010 . – 114 с.

Інформаційні ресурси

1. Захист інформації – [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації.
2. Комплексні системи захисту інформації / [Електронний ресурс]. [Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін]– Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

3. Технології захисту інформації [Електронний ресурс, URL: <http://umm.pstu.edu/handle/123456789/7947>] : методичні вказівки до самостійного вивчення дисципліни «Технології захисту інформації» для студентів напряму підготовки 6.050101 «Комп'ютерні науки» всіх форм навчання / уклад. С. В. Альшин. – Маріуполь : ПДТУ, 2015. – 37 с.

4. Ахрамович В. М. Навчальна програма дисципліни «Технології захисту інформації» (для спеціалістів) [Електронний ресурс, URL: http://library.iapm.edu.ua/metod_disc/pdf/4086up.pdf]. – К.: ДП «Вид. дім «Персонал», 2012. – 16 с.

5. Єгоров А.О. Методичні вказівки до виконання лабораторних робіт з дисципліни «Технології захисту інформації» [Текст], [Електронний ресурс, URL: <http://repository.dnu.dp.ua:1100/upload>] / А.О. Єгоров, Н.О. Соколова – Д.: НМетАУ, 2014. – 85 с.