Приватний вищий навчальний заклад
«Буковинський університет»
Факультет інформаційних технологій та економіки
Кафедра комп'ютерних систем і технологій

СХВАЛЕНО
на засіданні науково-методичної
ради факультету
протокол № 1 від 26 серпня 2025 р.

ЗАТВЕРДЖУЮ
Декан факультету ІТЕ
_____/ Тетяна ШТЕРМА/
«___» _____ 2025 р.

СИЛАБУС

обов'язкової навчальної дисципліни

«Технології захисту інформації»

Освітньо-професійна програма: Комп'ютерні науки

Спеціальність: Комп'ютерні науки

Галузь знань: Інформаційні технології

Рівень вищої освіти: перший (бакалаврський)

Факультет: Інформаційних технологій та економіки

Мова навчання: українська

Розробник: Гаць Богдан Миколайович – кандидат технічних наук, доцент

Профайл викладача: *https://bukuniver.edu.ua/university/faculties-and-departments/ite-faculty/department-of-computer-systems-and-technologies/*

E-mail: gatsbn@gmail.com

Консультації: четвер з 10.00 до 16.00.

1. **Анотація (призначення навчальної дисципліни).**

Освітній компонент «**Технології захисту інформації**» є складовою навчального плану підготовки фахівців першого (бакалаврського) рівня вищої освіти галузі знань **Інформаційні технології** спеціальності **Комп'ютерні науки**, побудована відповідно до вимог Європейської кредитної трансферно-накопичувальної системи (ECTS) і містить 5 кредитів. Форма підсумкового контролю – екзамен.

Предметом вивчення курсу «Технології захисту інформації» є комплекс методів, технологічних засобів та програмних інструментів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних у сучасних комп'ютерних системах і мережах. Процес вивчення охоплює освоєння криптографічних алгоритмів, протоколів безпечної передачі інформації, методів автентифікації та ідентифікації, а також технологій виявлення та запобігання несанкціонованому доступу до інформаційних ресурсів.

Важливою складовою предмета курсу є аналіз вразливостей програмно-апаратних комплексів та розробка стратегій захисту як структурованих, так і слабоструктурованих даних від сучасних кіберзагроз. Навчання спрямоване на формування у здобувачів освіти критичного розуміння принципів побудови захищених систем, що дозволяє ефективно впроваджувати технології безпеки при розв'язанні складних прикладних задач у професійній діяльності фахівця з комп'ютерних наук.

Особливе місце в предметі дисципліни займає вивчення міжнародних стандартів та нормативно-правової бази інформаційної безпеки, що закладає фундамент для прийняття обґрунтованих технічних рішень. Це забезпечує здатність майбутнього бакалавра адаптувати системи захисту до мінливих умов експлуатації та нових типів цифрових загроз протягом усього професійного життя.

2. **Мета та завдання вивчення дисципліни.**

Мета курсу – освоєння студентами теоретичними і практичними основами сучасних технологій захисту інформації від порушення її конфіденційності, цілісності та автентичності.

Завдання дисципліни – збереження цінності інформаційних ресурсів для їх власника. Збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Вивчення та засвоєння основних принципів проектування та побудови захищених систем і оцінки їх надійності.

Основні знання та вміння, яких набуває студент після опанування цієї дисципліни

Основні знання:

- мета та основні завдання захисту інформації, категорії інформаційної безпеки, класифікацію загроз інформаційної безпеки;
- типи політик безпеки розмежування доступу, методи захисту інформації, абстрактні моделі захисту інформації;
- шкідливе програмне забезпечення та методи протидії;
- технології захисту комп'ютерних мереж;
- методи криптографічного захисту інформації на основі симетричних криптосистем;
- блокові алгоритми та режими їх роботи;
- алгоритми сучасного блокового шифрування;
- генератори псевдовипадкових чисел та алгоритми потокового шифрування;
- алгоритми асиметричного шифрування;
- методи забезпечення цілісності даних та аунтефікації повідомлень;
- криптографічні хеш-функції стиснення, на основі блокового шифру;
- схеми цифрового підпису;
- протоколи ідентифікації та аутентифікації;
- протоколи розподілу ключів.

Основні вміння:

- здатність аналізувати та вибирати методи захисту інформації підприємства, будувати політику безпеки;
- реалізовувати захист інформації за допомогою симетричного блокового та потокового шифрування;
- застосовувати алгоритми асиметричного шифрування для забезпечення конфіденційності, цілісності та автентичності інформації;
- створювати електронний цифровий підпис.

Предметом вивчення навчальної дисципліни є вивчення основ та інформаційно-технологічних рішень захисту інформації.

3. Пререквізити:

- ОК12 Теорія ймовірності та математична статистика;

- ОК17 Комп'ютерна схемотехніка та архітектура комп'ютерів;
- ОК18 Організація баз даних та знань;
- ОК22 Об'єктно-орієнтоване програмування;
- ОК26 Комп'ютерні мережі.

4. Компетентності та результати навчання.

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

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов і вимог.

Загальні компетентності (ЗК)

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК11. Здатність приймати обґрунтовані рішення.

Спеціальні (фахові, предметні) компетентності

СК3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проєктування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.
СК8. Здатність проєктувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальнення, об'єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління.
СК13. Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж.
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Програмні результати навчання

РН5. Проектувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій.
РН9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук.
РН13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.
РН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

5. Зміст навчальної дисципліни

Змістовий модуль 1.

Тема 1. Фундаментальні засади інформаційної безпеки: класифікація загроз, модель порушника та формування політики захисту.
Тема 2. Методології захисту інформації.
Тема 3. Шкідливе програмне забезпечення та захист від нього.
Тема 4. Елементарна криптографія.
Тема 5. Сучасні алгоритми блокового шифрування.

Змістовий модуль 2.

Тема 6. Потокові шифри.
Тема 7. Математичний апарат криптографічного захисту: теорія чисел та алгоритми тестування простоти.
Тема 8. Криптосистеми з відкритим ключем.
Тема 9. Цілісність даних та аунтефікація повідомлень.

Тема 10. Протоколи ідентифікації та аутентифікації.

6. Система контролю та оцінювання.

Методи навчання:

- словесні методи (лекція, дискусія, пояснення, розповідь);
- практичні методи (практичні/лабораторні заняття, практичні завдання);
- наочні методи (демонстрація, ілюстрація, презентація);
- робота з інформаційними ресурсами: з навчально-методичною, науковою, нормативною літературою та інтернет-ресурсами;
- самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни;
- дистанційне навчання з використанням відповідних онлайн-платформ.

Форми та методи оцінювання:

- усне опитування;
- тестування;
- презентація результатів виконаних завдань;
- виконання вправ;
- контрольні роботи;
- підсумковий контроль –екзамен.

Поточний контроль проводиться на кожному практичному занятті.

Об'єктом поточного контролю знань студентів є:

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

Підсумковий контроль знань проводиться у формі екзамена.

На екзамен виносяться вузлові питання дисципліни та типові задачі, що потребують творчої відповіді та уміння синтезувати отримані знання і застосувати їх при вирішенні практичних задач. Максимально можлива оцінка за екзамен – 30 балів.

Семестрова кількість балів може становити від 0 до 100 балів і визначається як сума балів: отриманих за всі види роботи на практичних та лабораторних заняттях; за виконання самостійної роботи; модульних контрольних робіт, результат підсумкового контролю у формі екзамена.

Оцінювання здійснюється за національною шкалою – «відмінно», «добре», «задовільно», «незадовільно» та за шкалою ECTS.

Шкала оцінювання: національна та ЄКТС

Оцінка за шкалою ЄКТС	Оцінка за шкалою, що використовується у закладі вищої освіти та фахової передвищої освіти	Оцінка за національною шкалою
A	90-100	5 (відмінно)
B	80-89	4 (добре)
C	70-79	
D	60-69	3 (задовільно)
E	50-59	
FX	35-49	2 (незадовільно) з можливістю повторного складання
F	1-34	2 (незадовільно) з обов'язковим повторним вивченням дисципліни

Розподіл балів з навчальної дисципліни

Поточний контроль (аудиторна та самостійна робота)		Іспит	Загальна кількість балів
Модуль I	Модуль II		
35	35	30	100

Політика академічної доброчесності

Студент зобов'язаний ознайомитися з Положенням про забезпечення академічної доброчесності у ПВНЗ «Буковинський університет» та неухильно його дотримуватися. Текст документа розміщено у відкритому доступі на офіційному сайті університету. В освітньому процесі студент має виявляти дисциплінованість, ввічливість, доброзичливість, чесність і відповідальність.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації. Списування (копіювання тексту) під час виконання письмових робіт заборонені. Самостійні роботи у вигляді рефератів, доповідей, презентацій повинні мати коректні текстові посилання на використані інформаційні джерела. Дозволяється використання інструментів штучного інтелекту за умови дотримання принципів академічної доброчесності.

7.Рекомендована література

1. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Х.: Новий світ-2000, 2022. – 678 с.
2. Гаць Б. Використання блокчейн-технологій для забезпечення кібербезпеки в комп'ютерних системах / Боднарук О., Гаць Б., Осадчук С. / Наука і техніка сьогодні, 2024. № 9(37). С. 574 - 589.
3. Супрун О. М., Бойко О. Р., Гаць Б. М. Стеганографічні підходи до збереження метаданих у зображеннях для підвищення безпеки архівів // Зб. наук. пр. НУК. — 2025. — № 3 (501). — С. 182–189. — DOI: 10.15589/znp2025.3(501).22
4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с.
5. Бернакевич І.Є. Захист інформації [Електронний ресурс]. Режим доступу: http://e-learning.lnu.edu.ua/course/view.php?id=3009
6. Thakur K., Pathan A. S. K., Ismat S. (Eds.) Emerging ICT Technologies and Cybersecurity [Електронний ресурс] : From AI and ML to Other Futuristic Technologies / Kutub Thakur, Al-Sakib Khan Pathan, Sadia Ismat. – Cham : Springer, 2023. – URL: https://link.springer.com/book/10.1007/978-3-031-27765-8
7. Демчинський В. В., Грайворонський М. В., Кіреєнко О. В. Основи технологій захисту інформації [Електронний ресурс] : навчальний посібник / В. В. Демчинський, М. В. Грайворонський, О. В. Кіреєнко. – Kyiv : KPI, 2022. – URL: https://ela.kpi.ua/bitstream/123456789/53203/1/OTZI_Practices_plan_v115.pdf

Web-ресурси:

1. OWASP Foundation. OWASP Cheat Sheet Series [Електронний ресурс]. – URL: https://cheatsheetseries.owasp.org/ – набір кращих практик захисту веб-додатків.
2. NIST. Computer Security Resource Center (CSRC) [Електронний ресурс]. – URL: https://csrc.nist.gov/ – стандарти, керівництва та публікації з інформаційної безпеки.
3. MITRE. ATT&CK® – Adversarial Tactics, Techniques, and Common Knowledge [Електронний ресурс]. – URL: https://attack.mitre.org/ – знання про тактики та методи кіберзагроз.
4. CISA. Cybersecurity and Infrastructure Security Agency [Електронний ресурс]. – URL: https://www.cisa.gov/cybersecurity – довідкові матеріали та рекомендації з кібербезпеки.
5. Sans Institute. SANS Reading Room [Електронний ресурс]. – URL: https://www.sans.org/white-papers/ – колекція статей та аналітичних матеріалів з інформаційної безпеки.
6. ISO. ISO/IEC 27000 Family – Information Security Management Systems [Електронний ресурс]. – URL: https://www.iso.org/isoiec-27001-information-security.html – огляд стандартів ISO з інформаційної безпеки.
7. Cybersecurity & Infrastructure Security Agency – Shields Up [Електронний ресурс]. – URL: https://www.cisa.gov/shields-up – офіційна сторінка з рекомендаціями та матеріалами щодо підвищення кібербезпеки у рамках кампанії «Shields Up»
https://www.cisa.gov/shields-up – довідкова інформація про захист інформації для громадськості.}