Чернівецький національний університет імені Юрія Федьковича
Інститут фізико-технічних та комп'ютерних наук
Кафедра програмного забезпечення комп'ютерних систем

СИЛАБУС
навчальної дисципліни

«Інформаційна безпека бізнесу»

(вибіркова)

Освітньо-професійна програма «Інформаційні системи та технології»

Спеціальність 126 – Інформаційні системи та технології

Галузь знань 12 – Інформаційні технології

Рівень вищої освіти перший бакалаврський

Мова навчання українська

Розробник: доктор фіз.-мат.наук, професор, завідувач кафедри програмного забезпечення комп'ютерних систем Остапов Сергій Едуардович

Профайл викладача:
https://sites.google.com/chnu.edu.ua/pzks/%D0%BF%D1%80%D0%BE-%D0%BD%D0%B0%D1%81/%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D0%BA%D0%B8/%D0%BE%D1%81%D1%82%D0%B0%D0%BF%D0%BE%D0%B2-%D1%81-%D0%B5

Контактний тел. +38(0372)509 434
E-mail: s.ostapov@chnu.edu.ua

Сторінка курсу в Moodle:
https://moodle.chnu.edu.ua/course/view.php?id=962

Консультації: Очні та онлайн-консультації – згідно з графіком

1. **Анотація дисципліни**:

Навчальна дисципліна «Інформаційна безпека бізнесу» призначена для формування у студентів знань, вмінь та навичок з сучасних методів та засобів інформаційної безпеки, які будуть корисними при розгортання та обслуговуванні інформаційних систем сучасного бізнесу.

2. **Мета навчальної дисципліни**:

Надання студентам систематизованих знань з інформаційної безпеки сучасного бізнесу: мети, завдань, принципів організації комплексних систем електронної комерції та банківського бізнесу; забезпечити вмінням боротьби із загрозами інформації; теоретичними і практичними знаннями засобів захисту інформації, специфічних для комерційно-банківського сектору; методами боротьби з несанкціонованим доступом до інформації з обмеженим доступом, у тому числі комерційного характеру; використанням програмно-апаратних методів для побудови систем захисту.

Завдання дисципліни:

Випливають з ролі дисципліни у системі підготовки спеціалістів: вивчення студентами основних теоретичних понять захисту інформації; уміння застосовувати їх для розв'язку завдань, що ставить перед ними виробництво; набуття студентами практичних навичок; вільне володіння основними методами захисту інформації; розуміння основних понять і сучасного стану даного предмету.

3. **Пререквізити**:

Студенти повинні опанувати знаннями з дисциплін: «Операційні системи», «Теорія алгоритмів та програмування», «Комп'ютерні мережі», «Безпека програм та даних».

4. **Результати навчання**: У результаті вивчення навчальної дисципліни студент повинен:

знати:

- найновіші досягнення в галузі інформаційної безпеки бізнесу;
- характеристики основних підсистем ідентифікації та аутентифікації;
- характеристики основних механізмів доступу, пов'язаних з особливостями сфери застосування;
- характеристики підсистем захисту основних захищених протоколів, у тому числі спеціалізованих;
- основні поняття безпеки мікропроцесорних карток;
- основні канали витоку інформації та методи боротьби з ним;
- основні поняття безпеки систем електронної комерції та платіжних систем;
- основні поняття у сфері криптовалют.

вміти:

- використовувати програмні, організаційно-адміністративні та технічні засоби захисту комерційної інформації;
- орієнтуватися в законодавчо-нормативній базі в галузі захисту інформації;
- правильно налагоджувати підсистеми захисту сучасних операційних систем;
- використовувати спеціалізовані підсистеми захисту протоколів передавання даних, в т.ч. спеціалізованих;
- правильно визначати та застосовувати критерії захищеності автоматизованих систем обробки комерційної інформації.

Під час вивчення даної дисципліни студенти набудуть:

Загальних компетентностей:

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальних (фахових, предметних) компетентностей:

КС 1. Здатність аналізувати об’єкт проектування або функціонування та його предметну область.

КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмноапаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп’ютерно-інтегрованих систем та системної мережної структури, управління ними.

КС 8. Здатність управляти якістю продуктів і сервісів інформаційних систем та технологій протягом їх життєвого циклу.

Програмними результатами навчання є:

ПРН2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв’язанні задач проектування і використання інформаційних систем та технологій.

ПРН3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання інформаційних систем та технологій.

ПР 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

ПРН7. Обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій.

5. Опис навчальної дисципліни

5.1. Загальна інформація

Назва навчальної дисципліни: «Інформаційна безпека бізнесу»													
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**							**Вид підсумкового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**		
Денна	4	8	4	120		26			26	68			залік

5.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Традиційна та електронна комерція												
Тема 1.1. Вступ. Основні поняття електронної комерції та банкінгу	14	2		2		10						
Тема 1.2. Гроші та платіжні системи	18	4		4		10						

Тема 1.3. Електронна комерція типу B2B та системи обміну даними.	22	6		6		10						
Разом за змістовим модулем 1	**54**	**12**		**12**		**30**						
Змістовий модуль 2. Комп'ютерний захист фінансової інформації												
Тема 2.1. Віддалені платежі за допомогою банківських карток.	16	2		4		10						
Тема 2.2. Захищені протоколи	16	2		4		10						
Тема 2.3. Безпека мікропроцесорних карток	19	6		3		10						
Тема 2.4. Сучасні криптовалюти.	15	4		3		8						
Разом за змістовим модулем 2	**66**	**14**		**14**		**38**						
Усього годин	**120**	**26**		**26**		**68**						

5.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вивчення системи захисту даних TrueCrypt (BetaCrypt)	2
2	Вивчення системи захисту даних Криптобанк	4
3	Дослідження захисту інформації у спрощених EDI-системах	4
4	Розробка системи "Банкоматик"	4
5	Використання електронних гаманців у системах е-торгівлі	4
6	Вивчення захисту повідомлень у спрощеному протоколі SET	4
7	Розробка навчальної криптовалюти. Частина 1.	2
8	Розробка навчальної криптовалюти. Частина 2.	2
	Разом	26

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Створення спрощеної системи захисту протоколів iКР.	10
2	Розробка спрощеної версії механізмів захисту протоколу SET.	10
3	Розробка спрощеної версії системи мобільної торгівлі.	10
4	Розробка спрощеної версії системи електронних гаманців.	10
5	Емуляція роботи смарт-картки на основі флеш-накопичувача. Розробка спрощеної системи цифрової готівки.	10
6	Розробка спрощеної системи цифрової готівки.	8
7	Емуляція системи захисту смарт-картки.	10
	Разом	68

5.5. Індивідуальні завдання

Індивідуальні завдання включають: вивчення роботи програм для електронної комерції; розробку ПЗ, яке здійснює додатковий захист інформації в системах електронної торгівлі; вивчення роботи програм для відновлення інформації при транзакціях.

6. Система контролю та оцінювання

Види та форми контролю

Формами поточного контролю при вивченні курсу є:

- Усна відповідь студентів під час опитування на лекціях;
- Захист лабораторних робіт;
- Тестування з використанням платформи Moodle;
- Написання та захист рефератів.

Формами підсумкового контролю служать:

- Іспит;
- Залік, якщо він перебачений освітньою програмою.

Засобами оцінювання є:

- Модульні та поточні контрольні роботи;
- Тестувальна система на платформі Moodle;
- Реферати з тематики курсу;
- Виконання та захист лабораторних робіт.

Критерії оцінювання результатів навчання з навчальної дисципліни

Поточне тестування та самостійна робота							Кількість балів (залік)	Сума
Змістовий модуль 1			Змістовий модуль 2					
Т1.1	Т1.2	Т1.3	Т2.1	Т2.2	Т2.3	Т2.4	30	100
8	10	12	10	10	10	10		

7. Рекомендована література

Базова

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.:ВНV, 2009. – 608 с.
2. Остапов С.Е., Жихаревич В.В., Добровольський Ю.Г. Сучасні методи та засоби захисту інформації. Монографія. Чернівці : ЧНУ, 2021. 71 С.
3. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник. “Новий світ-2000”, 2019. 678 с.
4. Тарнавський Ю.А. Технології захисту інформації : підручник. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
5. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Чернівці : Родовід, 2015. 438 с.

Допоміжна

1. Y. Tanasyuk, S. Ostapov. Development and Research of Cryptographic Hash Functions Based on Two-Dimentional Cellular Automata//Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2018. – 8 (1), PP.24-27.
2. S. Ostapov, O. Val, S. Yanushevsky, D. Chyzhevsky. Cryptography on the Base of Cellular Automata // Internet in the Information Society. Monograph / Publisher: Scientific Publishing University of Dabrowa Gornicza, Editors: Maciej Rostanski, Piotr Pikiewicz, Pawel Buchwald, 2015. – pp.71-86.
3. Захист інформації в комп’ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко. Х. : НТУ “ХПІ”, 2014. 251с.
4. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.
5. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. / Б.А. Кормич. – К. : Кондор, 2008. – 382 с
6. Закон України “Про захист інформації в автоматизованих системах”
7. Закон України “Про інформацію”

8. Закон України “Про державну таємницю”

8. Інформаційні ресурси

1. Український центр інформаційної безпеки . – Електронний ресурс. – http://www.bezpeka.com
2. Системи керування базами даних: MS SQL Server, InterBase/FireBird, MySQL, Oracle