МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ
підготовки здобувачів освіти
першого (бакалаврського) рівня

спеціальності 122 Комп'ютерні науки

освітньо-професійної програми

Комп'ютерні науки та інформаційні технології

Луцьк – 2022

Силабус нормативного освітнього компонента «Технології захисту інформації» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 122 Комп'ютерні науки, за освітньою програмою Комп'ютерні науки та інформаційні технології.

Розробники Лаптєв О. А., професор кафедри комп'ютерних наук та кібербезпеки, д.т.н., снс.
Гаращенко В. В., ст. викладач кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:

 Гришанович Т. О.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 29 вересня 2022 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">12 Інформаційні технології
122 Комп’ютерні науки
Комп’ютерні науки та інформаційні технології
бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 1</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120 / 4</td><td>Семестр 8-ий</td></tr>
<tr><td>Лекції 20 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні 30 год.</td></tr>
<tr><td>Самостійна робота 62 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></td></tr>
</table>

ІІ. Інформація про викладача

ПІП Лаптєв Олександр Анатолійович
Науковий ступінь доктор технічних наук
Вчене звання - снс
Посада професор
Контактна інформація alaptev64@ukr.net
Дні занять http://194.44.187.20/

ПІП Гаращенко Володимир Володимирович
Посада старший викладач
Контактна інформація vg@socprime.com
Дні занять http://194.44.187.20/

ІІІ. Опис освітнього компонента

1. Анотація курсу. Освітній компонент “Технології захисту інформації” орієнтований на набуття теоретичних і практичних знань в області технологій захисту інформації, на ознайомлення здобувачів із концепціями сучасних методів захисту інформації. Основу курсу складають організаційно-правові, інженерно технічні та апаратно-програмні аспекти захисту інформації. Головна функція технології захисту інформації-забезпечення конфіденційності, цілісності та доступності інформації.

2. Мета і завдання освітнього компонента: є вивчення теоретичних основ та практичних аспектів використання технологій захисту інформації для вирішення сучасних задач з захисту інформації, оволодіння концепціями сучасних методів та технологій захисту інформації на об’єктах інформаційної діяльності та у автаматизованих системах обробки інформації

3. Результати навчання.

Загальні компетентності:

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК11. Здатність приймати обґрунтовані рішення.
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

IV. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Організаційні та інженерно – технічні аспекти технології захисту інформації						
Тема 1. Вступ до системи та технології захисту інформації	6	2		4		
Тема 2. Правові підстави та основні положення щодо створення комплексу ТЗІ в Україні	10	2	2	4	2	Звіт по лаб. роботі/2
Тема 3. Організаційно-правові аспекти технологій захисту інформації	10	2	2	6		Звіт по лаб. роботі/2
Тема 4. Захист інформації в АС від витоку технічними каналами	10	2	2	6		Звіт по лаб. роботі/4
Разом за модулем 1	36	8	6	20	2	**8**
Змістовий модуль 2. Апаратно-програмні технології захисту інформації.						
Тема 1. Апаратні технології захисту інформації	10	2	2	6		Звіт по лаб. роботі/2
Тема 2. Захист інформації в АС від руйнування каналами спеціального впливу.	14	2	4	8		Звіт по лаб. роботі/6
Тема 3. Технології програмного захисту інформації.	12	2	4	6		Звіт по лаб. роботі/4
Тема 4. Криптографічні технології захисту інформації у АС.	16	2	4	8	2	Звіт по лаб. роботі/6
Тема 5. Технології захисту від шкідливого коду.	18	2	6	8	2	Звіт по лаб. роботі/8
Тема 6. Перспективні напрями розвитку комплексу ЗІ в розподілених обчислювальних середовищах.	14	2	4	6	2	Звіт по лаб. роботі/6
Разом за модулем 2	84	12	24	42	6	**32**
Види підсумкових робіт						Бал
Тестування						30
Модульна контрольна робота 1						15

Модульна контрольна робота 2						15
Всього годин/Балів	120	30	36	46	8	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

2. Завдання для самостійного опрацювання.

   Самостійна робота здобувачів включає в себе:

   Опрацювання лекційного матеріалу. 8 год

   Перевірка здійснюється під час лабораторних занять та оцінюється при виставленні оцінки за змістовий модуль.

   Підготовка до практичних занять, виконання домашніх завдань. 8 год

   Перевірка здійснюється під час практичних занять.

   Систематизація вивченого матеріалу перед іспитом. 6 год
   Перевірка здійснюється під час іспиту.

   Вивчення тем, що не розглядаються в курсі лекцій. 40 год
   Перевірка здійснюється під час модульних контрольних заходів і оцінюється відповідною кількістю балів.

№ з/п	Тема	Кількість годин
1	Системи та технології захисту інформації	4
2	Правові підстави та основні положення щодо створення комплексу ТЗІ в Україні	4
3	Організаційно-правові аспекти технологій захисту інформації	6
4	Захист інформації в АС від витоку технічними каналами	6
5	Апаратні технології захисту інформації	6
6	Захист інформації в АС від руйнування каналами спеціального впливу.	8
7	Технології програмного захисту інформації.	6
8	Криптографічні технології захисту інформації у АС.	8
9	Технології захисту від шкідливого коду.	8
10	Перспективні напрями розвитку комплексу ЗІ в розподілених обчислювальних середовищах.	6
	Всього	62

IV. Політика оцінювання

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури;

підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна під час лабораторних робіт або під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати питання викладачу. Перескладання контрольних робіт та тестувань заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

V. Підсумковий контроль

Підсумковий контроль з даної дисципліни передбачено у вигляді заліку.

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, контрольних, тестових робіт та виконання індивідуального завдання. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 100 балів. Залік виставляється за результатами поточної роботи за умови, що здобувач освіти виконав усі види навчальної діяльності, визначеної силабусом освітнього компонента.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та здати завдання. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час семестру.

Якщо протягом семестру здобувач освіти набрав менше, ніж 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів, яку може отримати здобувач під час ліквідації академічної заборгованості, становить 100. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонента.

Визнання результатів навчання з паралельних та розподілених обчислень, які отримані у формальній освіті, здійснюється згідно «Положення про визнання результатів

навчання, отриманих у формальній, неформальній та/або інформальній освіті у ВНУ імені Лесі Українки» (https://cutt.ly/yNUt5Y4).

Питання для ліквідації заліку

1. Кіберзахист та захист інформації у чому різниця?
2. Модель захисту інформації.
3. Канали витоку інформації.
4. .Побудова і структура критеріїв захищеності інформації
5. Критерії конфіденційності, цілісності, доступності, спостереженості
6. Оцінка коректності реалізації послуг безпеки (критерії гарантій)
7. Основні складові захисту інформації.
8. Організаційно-правові аспекти захисту інформації.
9. Інженерно технічні напрямки захисту інформації.
10. Апаратно–програмні методи захисту інформації.
11. Антивірусні програми.
12. Спеціалізовані програмні засоби
13. Міжмережеві екрани.
14. Proxy-servers.
15. Віртуальна приватна мережа. Концепція побудови.
16. Системи виявлення вторгнень.
17. Системи запобігання вторгнень.
18. Аналіз мережевої безпеки.
19. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів.
20. Побудова системи антивірусного захисту корпоративної мережи.
21. Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації.
22. Відновлення даних з різних носіїв інформації.
23. Аудит і моніторинг безпеки.

VI. Шкала оцінювання

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VI. Рекомендована література та інтернет-ресурси.

Основна література

1. Закон України. Про захист інформації в інформаційно-телекомунікаційних системах. Введено в дію постановою Верховної Ради України від 05.07.94 р. № 81/94-ВР.
2. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
3. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави".
4. НД ЗІ 1.1-001-99. – Технічний захист інформації на програмно-керованих автоматичних телефонних станціях загального користування. Основні положення. Затверджений наказом ДСТСЗІ СБУ от від 28.04.99 р. № 22. Діє від 01.07.99.
5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ от 28.04.99 № 22. Діє від 01.07.99.
6. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ от 28.04.99 № 22. Діє від 01.07.99.
7. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
8. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.
9. НД ТЗІ 2.5-002-99. – Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28.04.99 № 22. Діє від 01.07.99.
11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
12. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від НСД під час оброблення в АС класу 2 (нетаємно). Затверджений наказом ДСТСЗІ СБУ від 13.12.2002 № 84.
13. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації Web-сторінки від несанкціонованого доступу Затверджений наказом ДСТСЗІ СБУ от від 02.04.03 № 33. Діє від 15.04.03.
14. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
15. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі Затверджено наказом ДСТСЗІ СБ України від 08.11.05.

16. ISO/IEC 7498-2, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. – Switzeland, 1989. – 32 p.
17. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
18. ISO/IEC 14888-3 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.
19. ITU-T Recommendation X.509. Information Technology – Open Systems Interconnection – The Directory Public Key and Attribute Certificate.
20. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.
21. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.
22. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assuracce requirements, 1999. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.
23. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. - К. : Центр навч.-наук, та наук.-пр. видань НА СБ України, 2014. - 190 с.
24. O.Laptiev, V.Savchenko, G.Shuklin, O.Stefurak. Detection and blocking of means of illegal obtaining of information at objects of information activity.Kyiv. SUT. 2020. – p.125 https://dut.edu.ua/ua/lib/1/category/737/view/2034
25. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020– 126 с. https://dut.edu.ua/ua/lib/2/category/96/view/2031
26. О.А. Лаптєв. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. Міленіум. 2020 – 326 с. УДК 004.056.53. ISBN 987-966-8063-79-3. https://www.dut.edu.ua/uploads/l_2162_16683938.pdf

Додаткові рекомендовані джерела

27. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, – 340 с.
28. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.