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
Програмні та програмно-апаратні комплекси ЗЗІ
першого (бакалаврського) рівня
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми
Кібербезпека та захист інформації

Луцьк – 2024

Силабус освітнього компонента «Програмні та програмно-апаратні комплекси ЗЗІ» підготовки бакалавра, галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробники:
Лаптєв О. А., професор кафедри комп'ютерних наук та кібербезпеки, доктор технічних наук, старший науковий співробітник.
Гришанович Т. О., доцент кафедри комп'ютерних наук та кібербезпеки, к.ф.-м.н.

Погоджено
Гарант освітньо-професійної програми: Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри: Гришанович Т. О.

1.Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність,

освітня програма,</th><th>Характеристика освітнього компонента</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="4">12 Інформаційні технології
125 Кібербезпека та захист інформації
Кібербезпека та захист інформації бакалавр</td><td>Нормативна</td></tr>
<tr><td rowspan="3">Кількість годин/кредитів 120/4</td><td>Рік навчання 4</td></tr>
<tr><td>Семестр_8-ий</td></tr>
<tr><td>Лекцій: 28 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td></td><td>Лабораторні роботи : 44год.</td></tr>
<tr><td></td><td>Самостійна робота 40 год.</td></tr>
<tr><td></td><td>Консультації: 8 год.</td></tr>
<tr><td colspan="3">Мова навчання: українська</td><td>Форма контролю: екзамен</td></tr>
</table>

II. Інформація про викладача

ПІП Лаптєв Олександр Анатолійович
Науковий ступінь: доктор технічних наук
Вчене звання: старший науковий співробітник
Посада: професор кафедри комп’ютерних наук та кібербезпеки
Контактна інформація : Alaptev64@ukr.net
Дні занять http://194.44.187.20/

ПІП Гришанович Тетяна Олександрівна
Науковий ступінь кандидат фізико-математичних наук
Посада доцент кафедри комп’ютерних наук та кібербезпеки
Контактна інформація hryshanovych.tatiana@vnu.edu.ua
Дні занять http://194.44.187.20/

III. Опис дисципліни

1. Анотація курсу. Освітній компонент «Програмні та програмно-апаратні комплекси ЗЗІ» відноситься до переліку дисциплін циклу професійної підготовки. Навчальна дисципліна присвячена підвищенню рівня знань здобувачів з теорії і практики забезпечення програмних та програмно-апаратних комплексів ЗЗІ, набуття вмінь і навичок зі створення надійного програмно та програмно-апаратного комплексу ЗЗІ, в знанні основ організації та порядку виконання робіт із застосування програмних та програмно-апаратних комплексів ЗЗІ.

2. Мета і завдання освітнього компонента: метою дисципліни «Програмні та програмно-апаратні комплекси ЗЗІ» є вироблення у студентів теоретичних знань та практичних навичок самостійної роботи з забезпечення програмних та програмно-апаратних комплексів ЗЗІ на об’єктах інформаційної діяльності. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і

організації програмних та програмно-апаратних комплексів ЗЗІ. Вивчення особливостей побудови безпеки інформаційно-комунікаційних систем на об'єктах критичної інфраструктури.

Результати навчання.

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні (фахові, предметні) компетентності

СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення

несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Нормативно-правові акти та теоретичні основи програмних та програмно-апаратних комплексів ЗЗІ.						
Тема 1. Загальні положення та вимоги в частині організації робіт із програмних та програмно-апаратних комплексів ЗЗІ.	7	2	2	2		ДС
Тема 2. Правові підстави та основні положення щодо програмних та програмно-апаратних комплексів ЗЗІ в Україні	9	2	4	4		ДС
Тема 3. Основи програмних та програмно-апаратних комплексів ЗЗІ.	8	2	4	2		Звіт по лаб. роботі
Тема 4. Безпека інформації. Захист інформації програмними та програмно-апаратними комплексами.	8	2	2	4		Звіт по лаб. роботі
Тема 5.Забезпечення безпеки інформації програмними комплексами ЗЗІ	7	2	4	2		Звіт по лаб. роботі
Тема 6. Захист інформації програмнимт та програмно-апаратними комплексами ЗЗІ	7	4	4	4		Звіт по лаб. роботі
Разом за модулем 1	56	14	20	22		30
Змістовий модуль 2. Побудова системи і основних програмних та програмно-апаратних комплексів ЗЗІ						
Тема 1. Технічне завдання на створення програмних та програмно-апаратних комплексів ЗЗІ.	6	2	2	2		Звіт по лаб. роботі/
Тема 2. Основи технічного захисту інформації в ІС.	10	2	4	6		Звіт по лаб. роботі
Тема 3. Особливості проектування програмних та програмно-апаратних комплексів ЗЗІ для АС різних класів. Оцінка ефективності.	10	2	2	6		Звіт по лаб. роботі
Тема 4. Перспективні напрями розвитку програмних та програмно-	11	4	4	8		Звіт по лаб. роботі

апаратних комплексів ЗЗІ						
Тема 5. Випробування та перевірка програмних та програмно-апаратних комплексів ЗЗІ	11	2	2	8		Звіт по лаб. роботі
Тема 6. Введення програмних та програмно-апаратних комплексів ЗЗІ в дію.	8	2	4	8		Звіт по лаб. роботі
Разом за модулем 2	64	14	18	24	8	30
Тестування						10
Модульна контрольна робота 1						10
Модульна контрольна робота 2						10
ІНДЗ						10
Всього годин/Балів	120	28	38	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.

1. Завдання для самостійного опрацювання.
Самостійна робота здобувачів включає в себе:

Опрацювання лекційного матеріалу. 10 год
Перевірка здійснюється під час лабораторних занять та оцінюється при виставленні оцінки за змістовий модуль.

Підготовка до лабораторних занять, виконання домашніх завдань. 14 год
Перевірка здійснюється під час лабораторних занять.

Систематизація вивченого матеріалу перед контрольними заходами, тестуванням. 6 год
Перевірка здійснюється під час контрольних заходів, тестування.

Вивчення тем, що не розглядаються в курсі лекцій. 16 год
Перевірка здійснюється під час модульних контрольних заходів і оцінюється відповідною кількістю балів.

№ з/п	Тема	Кількість годин
1	Правові підстави та основні положення щодо створення програмних та програмно-апаратних комплексів ЗЗІ в Україні	6
2	Основи програмних та програмно-апаратних комплексів ЗЗІ.	6
3	Технічний захист інформації програмними та програмно-апаратними комплексами ЗЗІ.	6

4	Захист інформації в АС програмними та програмно-апаратними комплексами ЗЗІ	6
5	Антивірусні програми. Спеціалізовані програмні засоби.	6
6	Системи виявлення вторгнень. Системи запобігання вторгнень.	6
7	Засоби аутентифікації користувачів і аналізу безпеки системи	5
8	Віртуальна приватна мережа. Концепція побудови.	5
	Всього	46

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. Завдання для практичного виконання (лабораторні роботи, ІНДЗ, самостійні роботи), завдання підсумкового контролю (тести, контрольні роботи, що передбачають розробку програм) здаються із використанням засобів дистанційного курсу.

Під час вивчення освітнього компонента можливе визнання інших результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

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. При виконанні лабораторних робіт з курсу здобувачі мають право використовувати власні ноутбуки, якщо вони підтримують необхідне програмне забезпечення.

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, матеріали дистанційного курсу "Технічні системи захисту інформації", розміщених на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи вищезазначені дистанційні курси, або під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу. Існує можливість використання форуму дистанційного курсу. Перескладання контрольних робіт та тестувань заборонено.

1. Підсумковий контроль

Підсумковою формою контролю освітнього компонента "Технічні системи захисту інформації" є іспит.

Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та підсумковий контроль (самостійне виконання індивідуальних завдань, контрольні роботи, перевірка теоретичної підготовки у формі тестування, ІНДЗ). Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 40 балів. Максимальна кількість балів, яку може отримати здобувач за підсумковий контроль за семестр складає 60 балів.

Якщо за результатами семестру накопичено не менше 75 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому випадку студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається.

Іспит передбачає виконання тестових завдань (10 питань по одному балу) та відповідь на питання (30 балів) Викладач залишає за собою право ставити уточнюючі питання під час відповіді студента та просити прокоментувати програмний код. Студент повинен використати засобі тієї мови програмування, яка вказана у завданні.

Питання для іспиту

1. Кіберзахист та захист інформації у чому різниця?
2. Модель захисту інформації.
3. Основні складові захисту інформації.
4. Організаційно-правові аспекти захисту інформації.
5. Інженерно технічні напрямки захисту інформації.
6. Апаратно–програмні методи захисту інформації.
7. Що вивчає дисципліна програмні методи захисту інформації?
8. Антивірусні програми.
9. Спеціалізовані програмні засоби
10. Міжмережеві екрани.
11. Proxy-servers.
12. Віртуальна приватна мережа. Концепція побудови.
13. Системи виявлення вторгнень.
14. Системи запобігання вторгнень.
15. Аналіз мережевої безпеки.

16. Критерії оцінки інформаційної безпеки та аспекти захисту інформації.
17. Засоби управління, збереження, доступу до паролів та правила роботи з ними.
18. Управління ідентифікацію і доступом.
19. Засоби аутентифікації користувачів і аналізу безпеки системи.
20. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів.
21. Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.
22. Комп'ютерні віруси і проблеми антивірусного захисту.
23. Побудова системи антивірусного захисту корпоративної мережи.
24. Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації.
25. Відновлення даних з різних носіїв інформації.
26. Аудит і моніторинг безпеки.
27. Порядок розроблення та оформлення програм і методик випробувань Що наводять у розділі "Вимоги щодо забезпечення охорони державної таємниці».
28. Завдання Служби захисту інформації.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є іспит

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

1. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
2. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).
3. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).
4. Закон України "Про захист інформаційно- телекомунікаційних системах". https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Закон України "Про інформацію". https://zakon.rada.gov.ua/laws/main/2657-12
6. Закон України "Про основні засади забезпечення кібербезпеки України" https://zakon.rada.gov.ua/laws/main/2163-19
7. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
8. ISO/IEC 14888-3 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.
9. 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.
10. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.
11. Лаптєв О.А., Кузавков В.В., Хорошко В.О. «Системи пошуку засобів негласного здобуття акустичної інформації» – К. Міленіум. 2023 – 282 с. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII

Додаткова література:

1. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
2. 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.
3. 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.
4. 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.

Додаткові джерела:

1. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.
2. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.