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

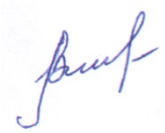
СИЛАБУС
нормативного освітнього компонента
СУЧАСНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Підготовки другого (магістерського) рівня вищої освіти
Спеціальності 122 Комп'ютерні науки
Освітньо-професійної програми Комп'ютерні науки та інформаційні технології

Луцьк – 2023

Силабус нормативного освітнього компонента «Сучасні технології забезпечення кібербезпеки в інформаційно-комунікаційних системах» підготовки магістрів, галузі знань 12 Інформаційні технології, спеціальності 122 Комп'ютерні науки, за освітньою програмою Комп'ютерні науки та інформаційні технології

Розробники:
Лаптєв Олександр Анатолійович, доктор технічних наук, старший науковий співробітник, професор кафедри комп'ютерних наук та кібербезпеки
Гаращенко Володимир Вікторович, старший викладач кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Булатецький В.В.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 28.09.2023 р.

Завідувач кафедри:  Гришанович Т. О.

© Лаптєв О.А., 2023 р.
© Гаращенко В. В., 2023 р.

І. Опис освітнього компонента

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Нормативна</td></tr>
<tr><td>Денна форма навчання</td><td rowspan="7">Галузь знань:
12 Інформаційні технології,
спеціальність:
122 Комп’ютерні науки,
освітньо-професійна програма:
Комп’ютерні науки та інформаційні технології,
освітній рівень: магістр.</td><td>Рік підготовки 2</td></tr>
<tr><td rowspan="3">Кількість
Годин/кредитів
120/4</td><td>Семестр 3</td></tr>
<tr><td>Лекції 14 год.</td></tr>
<tr><td>Лабораторні 20 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td>Самостійна робота 78 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
<tr><td colspan="3">Мова навчання – Українська</td></tr>
</table>

ІІ Інформація про викладачів

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;

ПІП: Гаращенко Володимир Вікторович
Посада: старший викладач кафедри комп’ютерних наук та кібербезпеки;
Контактна інформація: vg@socprime.com

Дні занять: http://94.130.69.82/cgi-bin/timetable.cgi.

ІІІ. Опис освітнього компонента

Анотація курсу. Силабус освітнього компонента «Сучасні технології забезпечення кібербезпеки в інформаційно-комунікаційних системах» складено відповідно до освітньо-професійної програми «Комп’ютерні науки та інформаційні технології» другого рівня вищої освіти, галузі знань 12 Інформаційні технології, за спеціальністю 122 Комп’ютерні науки. Освітній компонент «Сучасні технології забезпечення кібербезпеки в інформаційно-комунікаційних системах» належить до переліку нормативних освітніх компонент. Задача освітнього компонента полягає у підвищенні рівня знань студентів з теорії і практики захисту інформації, набуття вмінь і навичок з виявлення каналів витоку інформації, їх блокування, створенні, застосування механізмів захисту та оцінки рівня захищеності інформаційно-комунікаційних систем і технологій від несанкціонованого доступу до ресурсів. В знанні основ організації та порядку виконання робіт із створення захищених телекомунікаційних систем залежно від характеру об’єкта.

Мета і завдання освітнього компонента: надбання здобувачами загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації сучасних технологій забезпечення кібербезпеки в інформаційно-комунікаційних системах. Огляд практичних аспектів побудови моделі порушника та моделі загроз, вивчення проблем створення і реалізації політики захисту інформації програмними методами. Вивчення

особливостей захисту інформації програмними методами та побудова систем захисту інформаційних ресурсів з використання програмних методів захисту інформації.

Завдання курсу:

- забезпечення стабільних базових теоретичних знань, теорії і практики щодо управління інформаційною та кібернетичною безпекою на основі існуючих технологій та програмних продуктів, сприяти ефективному формуванню у здобувачів наступних професійних компетентностей;
- здатність брати участь в формуванні програмних методів захисту інформації та кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;
- здатність брати участь у проектуванні та розробці програмних методів захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури;
- здатність брати участь у проведенні контрольних заходів щодо визначення ефективності та результативності програмних методів захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури безпекою.

1. Перелік компетентностей випускника

Загальні компетентності

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК03. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК05. Здатність вчитися й оволодівати сучасними знаннями.

ЗК07. Здатність генерувати нові ідеї (креативність).

Спеціальні (фахові, предметні) компетентності

СК01. Усвідомлення теоретичних засад комп'ютерних наук.

СК02. Здатність формалізувати предметну область певного проєкту у вигляді відповідної інформаційної моделі.

СК03. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області.

СК04. Здатність збирати і аналізувати дані (включно з великими), для забезпечення якості прийняття проєктних рішень.

СК10. Здатність оцінювати та забезпечувати якість ІТ-проєктів, інформаційних та комп'ютерних систем різного призначення, застосовувати міжнародні стандарти оцінки якості програмного забезпечення інформаційних та комп'ютерних систем, моделі оцінки зрілості процесів розробки інформаційних та комп'ютерних систем.

СК11. Здатність ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп'ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом

Програмні результати навчання

РН1. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань.

РН2. Мати спеціалізовані уміння/навички розв'язання проблем комп'ютерних наук, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур.

РН6. Розробляти концептуальну модель інформаційної або комп'ютерної системи.

РН13. Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

РН15. Виявляти потреби потенційних замовників щодо автоматизації обробки інформації.

РН18. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

2. Структура освітнього компонента

№ п/п	Назва теми*	Кількість годин					Форма контролю / бали
		Усього	у тому числі				
			Лек.	Лаб.	Сам. роб.	Конс.	
Модуль 1. Нормативно-правові акти побудови програмних методів захисту інформації						2	Контрольна робота (МКР1,тест)/ 20 б.
1	Тема 1. Інформаційна безпека як процес управління ризиками сучасних ОІД. Тема 2. Забезпечення якості програмного забезпечення – основні поняття та визначення.	4	2		2		
2	Тема 3. Небезпечні програмні засоби, програми з ПН діянням та їх властивості.	10	2	2	6		Захист лаб. роботи/4 б.
3	Тема 4. Визначення та класифікація malicious software і програм з ПН впливом.	16	2	4	10		Захист лаб. роботи/8 б.
4	Тема 5. Модель якості програмного забезпечення за Макколом, Боемом, FURPS, Гецци, SATC та ін.	16	2	4	10		Захист лаб. роботи/8 б.
	Разом за змістовим модулем 1	48	8	10	28	2	
Модуль 2. Функціонування системи та основних підсистем методів захисту інформації						2	Контрольнар обота (МКР2 тест)/20 б.
5	Тема 6. Види якості програмного забезпечення.	8	2	2	4		Захист лаб. роботи/4 б.
6	Тема 7. Вплив Computer virus на програмно-апаратні засоби в інформаційно-телекомунікаційних системах.	20	2	4	12		Захист лаб. роботи/8 б.
7	Тема 8. Життєвий цикл програмного забезпечення. Типи та призначення моделей життєвого циклу програмного забезпечення Тема 9. Модель еволюційного прототипування життєвого циклу програмного забезпечення.	20	2	4	14		Захист лаб. роботи/8 б.
	Разом за змістовим модулем 2	48	6	10	30	2	
	ІНДЗ.	24			20	4	Захист ІНДЗ/20 б.
	Всього	**120**	**14**	**20**	**78**	**8**	**100 б.**

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	24
2	Опрацювання лекційного матеріалу. Робота з джерелами інформації.	14
3	Виконання ІНДЗ	20
4	Побудова системи технічних систем захисту інформації та систем управління інформаційною безпекою інформаційно-комунікаційної системи організації та її основних підсистем.	2
5	Основи організації технічних систем захисту інформації на підприємстві. Основи методичного забезпечення технічних систем захисту інформації в інформаційних системах. Основи побудови системи організації програмних методів захисту інформації на підприємстві. Основи організації захисту інформації у державі.	2
6	Основні концептуальні положення щодо побудови технічних систем захисту інформації; налагодження віддаленого доступу до комп'ютера. Критерії оцінки інформаційної безпеки та аспекти захисту інформації. Основні технічні засоби добування інформації. Засоби управління, збереження, доступу до паролів та правила роботи з ними.	2
7	Основні типи та загальний огляд комп'ютерних вірусів. Огляд найпоширеніших антивірусних програм та їх класифікація.	2
8	Огляд сучасних операційних систем, відновлення даних з різних носіїв інформації	2
	Разом	78

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.

Політика щодо академічної доброчесності. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація) викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську корпоративну пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на корпоративну електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі здобувачами.

Політика щодо перескладання. Перескладання контрольних робіт та тестувань, відбувається із дозволу лектора і тільки за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба,

академічна мобільність, які необхідно підтверджувати відповідними документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту. За об'єктивних причин навчання може відбуватись в он-лайн формі за погодженням з керівником курсу та деканом факультету.

Поєднання навчання та досліджень. Здобувачі вищої освіти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, зокрема, написання та опублікування наукових тез та статей з тематики дисципліни. За рішенням кафедри здобувачам, які брали участь у роботі конференцій, підготовці наукових публікацій, конкурсах студентських наукових робіт за тематикою ОК й досягли значних результатів, може бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю. Систему бонусних балів погоджує науково-методична комісія факультету інформаційних технологій і математики. При цьому загальна кількість балів, що вноситься до відомості за поточну роботу, у випадку ОК, де передбачено екзамен, не може перевищувати 40 б.

Визнання результатів навчання, отриманих у формальній, неформальній освіті. Під час вивчення освітнього компонента можливе визнання 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».

Підсумковий контроль

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль (нараховується за якісне виконання лабораторних робіт) та підсумковий модульний контроль (нараховується за виконання модульних контрольних робіт та модульних тестових робіт, до лекційних матеріалів курсу та виконання ІНДЗ). Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи, тестові завдання, ІНДЗ і складає 60 балів.

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому випадку здобувач складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів при цьому бали за підсумковий модульний контроль анульовуються.

Екзамен проходить в усній формі. Оцінка за семестр у випадку складання іспиту є сумою балів поточного контролю та балів, отриманих під час іспиту.

Питання, які виносяться на екзамен

1. Концептуальні основи побудови систем технічного захисту інформації.
2. Налагодження віддаленого доступу до комп'ютера.
3. Теоретичні основи технічних засобів захисту інформації.
4. Основи побудови технічних засобів добування інформації, що утворюють захищену систему технічного захисту інформації.
5. Засоби управління, збереження, доступу до паролів та правила роботи з ними.
6. Засобів аутентифікації користувачів і аналізу безпеки системи.
7. Побудову системи технічних систем захисту інформації та систем управління інформаційною безпекою інформаційно-комунікаційної системи організації та її основних підсистем.
8. Основи організації технічних систем захисту інформації на підприємстві.

9. Основи методичного забезпечення технічних систем захисту інформації в інформаційних системах.
10. Методи захисту інформації своєму призначенню.
11. Шкідливе програмне забезпечення.
12. Основи побудови системи організації програмних методів захисту інформації на підприємстві.
13. Основи організації захисту інформації у державі.
14. Основні типи та загальний огляд комп'ютерних вірусів.
15. Базові настроювання клієнтських та серверних операційних систем.
16. Поняття антивірусної програми.
17. Огляд найпоширеніших антивірусних програм та їх класифікація.
18. Криптографічний вид захисту інформації .
19. Відновлення даних з різних носіїв інформації.

Екзаменаційні білети складаються з комплексних завдань:

- теоретичні питання у розгорнутому вигляді та у вигляді тесту (60%)
- практичні завдання (40%)

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**
90 – 100	A	Відмінно
82 – 89	B	Добре
75 - 81	C	
67 -74	D	Задовільно
60 - 66	E	
1 – 59	Fx	Незадовільно

V. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНТЕРНЕТ-РЕСУРСИ

Основні рекомендовані джерела

Закон України. Про захист інформації в інформаційно-телекомунікаційних системах. Введено в дію постановою Верховної Ради України від 05.07.94 р. № 81/94-ВР.

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. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. НД ТЗІ 2.5-002-99. – Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

8. 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.
9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
10. 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.
11. 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.
12. 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.
13. 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.
14. ISO/IEC 7498-2, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. – Switzeland, 1989. – 32 p.
15. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
16. ISO/IEC 14888-3 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.
17. ITU-T Recommendation X.509. Information Technology – Open Systems Interconnection – The Directory Public Key and Attribute Certificate.
18. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.
19. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.
20. 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.
21. 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
22. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others. Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c. ISBN 978-617-7319-31-2 (on-line). ISBN 978-617-7319-32-9 (print). DOI: https://doi.org/10.15587/978-617-7319-31-2
23. О.А.Лаптєв, В.В.Собчук, О.М. Станжицький, Н.В Лукова-Чуйко. A comprehensive method of evaluating the effectiveness of the distance learning system in higher education institutions. In book : education, science, research during martial law. Collective monograph. Riga, Latvia : «Baltija Publishing», November 14, 2022. 374 p.(pp.209-231). DOI: https://doi.org/10.30525/978-9934-26-247-0-9
24. EDUCATION, SCIENCE, RESEARCH DURING MARTIAL LAW | Publishing House "Baltija Publishing". *Publishing House Baltija Publishingâ*. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/book/261/7241/15069-1.
25. Laptiev O., and other. Methodological aspect of ensuring state security in the mind threats. University of Security Management in Koshitze. Slovakia. 2023. 272 p. ISBN 978-80-8185-058-5. (Charter 10. pp.-137-150.)
26. Підтримка - Підтримка й завантаження продукції Cisco: документація, інструменти, заявки. *Cisco*. URL: https://www.cisco.com/c/uk_ua/support/index.html.
27. Ucci D., Aniello L., Baldoni R. Survey on the Usage of Machine Learning

28. Techniques for Malware Analysis // arXiv preprint arXiv:1710.08189. 2018.

Інформаційні ресурси

1. Навчальний та інформаційний сайт [Електронний ресурс]. – Режим доступу: http://uml.org/
2. Mcafee labs threats report. 2015. [Електронний ресурс]. – Режим доступу: https://scadahacker.com/library/Documents/Threat_Intelligence/McAfee%20-%20Threat%20Report%202015-2Q.pdf
3. Symantec intelligent report. 2015. [Електронний ресурс]. – Режим доступу: https://www.symantec.com/content/en/us/enterprise/other_resources/intelligence_report_05-2015.en-us.pdf
4. «CodeGuru:API Hooking Revealed» [Електронний ресурс]. – Режим доступу: http://www.codeguru.com/cpp/wp/system/misc/article.php/c5667/
5. [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua
6. [Електронний ресурс]. – Режим доступу: http://www.kiev-security.org.ua