

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
Безпека інформаційно-комунікаційних систем
першого (бакалаврського) рівня
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми
Кібербезпека та захист інформації

Луцьк – 2024

Силабус освітнього компонента «Безпека інформаційно-комунікаційних систем » підготовки бакалавра, галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробники:

Лаптев 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:  Черняшук 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.

@Лаптев О.А., 2024 р.

1.Опис освітнього компонента

Найменування показників	Галузь знань, спеціальність, освітня програма,	Характеристика освітнього компонента
Денна форма навчання	12 Інформаційні технології 125 Кібербезпека та захист інформації Кібербезпека та захист інформації бакалавр	Нормативна
Кількість годин/кредитів 120/4		Рік навчання 4
		Семестр_8-ий
		Лекцій: 28 год.
		Лабораторні роботи : 44год.
ІНДЗ: є		Самостійна робота 40 год.
		Консультації: 8 год.
		Форма контролю: екзамен
Мова навчання: українська		

II. Інформація про викладача

ППП Лаптев 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 <https://ps.vnu.edu.ua/cgi-bin/timetable.cgi>

III. Опис дисципліни

1. Анотація курсу. Освітній компонент «Безпека інформаційно-комунікаційних систем» відноситься до переліку дисциплін циклу професійної підготовки. Навчальна дисципліна присвячена підвищенню рівня знань здобувачів з теорії і практики забезпечення безпеки інформаційно-комунікаційних систем, набуття вмінь і навичок зі створення надійної безпеки інформаційно-комунікаційних систем, в знанні основ організації та порядку виконання робіт із безпеки інформаційно-комунікаційних систем.

2. Мета і завдання освітнього компонента: метою дисципліни «Безпека інформаційно-комунікаційних систем» є вироблення у студентів теоретичних знань та практичних навичок самостійної роботи з забезпечення безпека інформаційно-комунікаційних систем на об'єктах інформаційної діяльності. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації безпеки інформаційно-комунікаційних систем. Вивчення особливостей побудови безпека 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 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

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.

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 безпеки інформаційно-комунікаційних систем.						
Тема 1. Загальні положення та вимоги в частині організації робіт	7	2	2	2		ДС

із безпеки інформаційно-комунікаційних систем.						
Тема 2. Правові підстави та основні положення щодо безпеки інформаційно-комунікаційних систем в Україні	9	2	2	4		ДС
Тема 3. Основні положення про безпеку інформаційно-комунікаційних систем.	8	2	2	2		Звіт по лаб. роботі
Тема 4. Безпека інформації. Захист інформації від НСД.	8	2	2	4		Звіт по лаб. роботі
Тема 5. Забезпечення безпеки інформації від витоку технічними каналами	7	2	2	2		Звіт по лаб. роботі
Тема 6. Захист інформації від руйнування каналами спеціального впливу.	7	4	2	2		Звіт по лаб. роботі
Разом за модулем 1	56	14	12	20		30
Змістовий модуль 2. Побудова системи і основних підсистем безпеки інформаційно-комунікаційних систем						
Тема 1. Технічне завдання на створення безпеки інформаційно-комунікаційних систем.	6	2	2	2		Звіт по лаб. роботі/
Тема 2. Основи технічного захисту інформації в ІС.	10	2	2	6		Звіт по лаб. роботі
Тема 3. Особливості проектування ТЗІ для АС різних класів. Оцінка ефективності.	10	2	2	6		Звіт по лаб. роботі
Тема 4. Перспективні напрями розвитку безпеки інформаційно-комунікаційних систем	11	4	2	8		Звіт по лаб. роботі
Тема 5. Випробування та перевірка систем безпеки інформаційно-комунікаційних систем	11	2	2	8		Звіт по лаб. роботі
Тема 6. Введення системи безпеки інформаційно-комунікаційних систем в дію.	8	2	2	4		Звіт по лаб. роботі
Разом за модулем 2	64	14	12	20	8	30
Тестування						10
Модульна контрольна робота 1						10
Модульна контрольна робота 2						10
ІНДЗ						10
Всього годин/Балів	120	28	24	40	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.	10 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 безпеки інформаційно-комунікаційних систем в Україні	5
2	Основні положення про службу захисту інформації. Кібербезпека об'єктів критичної інфраструктури.	5
3	Технічний захист інформації інформаційно-комунікаційних системах .	5
4	Захист інформації в АС технічними засобами від руйнування каналами спеціального впливу.	5
5	Основи безпеки інформаційно-комунікаційних систем.	5
6	Перспективні напрями розвитку безпеки інформаційно-комунікаційних систем	5
7	Випробування системи технічного захисту інформації та його атестація	5
8	Особливості проектування безпеки інформаційно-комунікаційних систем різних класів. Оцінка ефективності.	5
	Всього	40

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); посилення 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 засоби тієї мови програмування, яка вказана у завданні.

Питання для іспиту

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. Сформулюйте основні концептуальні положення теорії захисту інформації.
9. Як впливають показники інформації, що захищається, на структуру і
10. Підходи до проектування системи захисту інформації?
11. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені.
12. Класифікація загроз інформаційної безпеки за характером впливу
13. Класифікація загроз інформаційної безпеки за розміщенням їх джерела. Які основні види загроз безпеки інформаційним технологіям?
14. Основні техногенні передбачувані та непередбачені загрози інформаційній системі
15. Яку систему складають дестабілізуючі чинники відповідно до технології і функціонування інформації?
16. Організаційно-правові аспекти захисту інформації.
17. Інженерно технічні напрямки захисту інформації.
18. Апаратно–програмні методи захисту інформації.
19. Які основні методи захисту інформації від НСД в автоматизованих системах?
20. Дайте характеристику основним та допоміжним технічним засобам та системам.
21. Розкрийте поняття зони 1, зони 2 та контрольованої зони.
22. Умови обробки інформації в системі.
23. Порядок розроблення та оформлення програм і методик випробувань. Що наводять у розділі “Вимоги щодо забезпечення охорони державної таємниці”.
24. 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. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).
2. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).
3. Закон України "Про захист інформаційно- телекомунікаційних системах". <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
4. Закон України "Про інформацію". <https://zakon.rada.gov.ua/laws/main/2657-12>
5. Закон України "Про основні засади забезпечення кібербезпеки України" <https://zakon.rada.gov.ua/laws/main/2163-19>
6. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с.
7. Лаптев 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_NEGLASNO_GO_ZDOBUTTA_AKUSTICNOI_INFORMACII
8. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
9. 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.
10. 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.