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
Технічний захист інформації
першого (бакалаврського) рівня
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми
Кібербезпека та захист інформації

Луцьк – 2024

Силабус освітнього компонента «Технічний захист інформації» 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.

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: 20 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td rowspan="3"></td><td>Лабораторні роботи : 24год.</td></tr>
<tr><td>Самостійна робота 68 год.</td></tr>
<tr><td>Консультації: 8 год.</td></tr>
<tr><td colspan="3">Форма контролю: екзамен</td></tr>
<tr><td colspan="3">Мова навчання: українська</td></tr>
</table>

ІІ. 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 https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

ІІІ. Опис дисципліни

1. Анотація курсу. Освітній компонент «Технічний захист інформації» відноситься до переліку дисциплін циклу професійної підготовки. Навчальна дисципліна присвячена підвищенню рівня знань здобувачів з теорії і практики захисту від витоку інформації технічними каналами, набуття вмінь і навичок з виявлення технічних каналів витоку інформації, їх блокування, створенні та впровадженні комплексів технічного захисту інформації, в знанні основ організації та порядку виконання робіт із систем захисту інформації від витоку інформації.

2. Мета і завдання освітнього компонента: метою дисципліни «Технічний захист інформації» є вироблення у студентів теоретичних знань та практичних навичок самостійної роботи з забезпечення технічного захисту інформації на об’єктах інформаційної діяльності. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації технічного захисту інформації. Вивчення особливостей побудови технічних систем захисту інформації та централізованого управління системою інформаційної безпеки.

1. **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 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності

СК 1. 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 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

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 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту 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 технічних систем захисту інформації.						
Тема 1. Загальні положення та вимоги в частині організації робіт із технічного захисту інформації.	7	1		6		ДС
Тема 2. Правові підстави та основні положення щодо створення комплексу ТЗІ в Україні	9	1	2	6		ДС
Тема 3. Основні положення про службу захисту інформації. Технічний захист інформації.	8	2	2	4		Звіт по лаб. роботі
Тема 4. Захист інформації від НСД.	8	2	2	4		Звіт по лаб. роботі
Тема 5.Захист інформації від витоку технічними каналами	7	1	2	4		Звіт по лаб. роботі
Тема 6. Захист інформації від руйнування каналами спеціального впливу.	7	1	2	4		Звіт по лаб. роботі
Тема 7. Порядок проведення робіт зі створення систем технічного захисту інформації.	10	2	2	6		Звіт по лаб. роботі
Разом за модулем 1	56	10	12	34		30
Змістовий модуль 2. Побудова системи і основних підсистем ТЗІ						
Тема 1. Технічне завдання на створення ТЗІ.	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 комплексу ТЗІ в кіберпросторі.	11	1	2	8		Звіт по лаб. роботі
Тема 5. Випробування та перевірка	11	1	2	8		Звіт по лаб.

технічного захисту інформації						роботі
Тема 6. Введення системи технічного захисту в дію.	8	2	2	4		Звіт по лаб. роботі
Разом за модулем 2	64	10	12	34	8	30
Тестування						10
Модульна контрольна робота 1						10
Модульна контрольна робота 2						10
ІНДЗ						10
Всього годин/Балів	120	20	24	68	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. 10 год
Перевірка здійснюється під час лабораторних занять та оцінюється при виставленні оцінки за змістовий модуль.

Підготовка до лабораторних занять, виконання домашніх завдань. 24 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. 28 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 комплексу ТЗІ в Україні	4
2	Основні положення про службу захисту інформації. Технічний захист інформації.	8
3	Технічний захист інформації в АС від НСД.	8
4	Захист інформації в АС технічними засобами від руйнування каналами спеціального впливу.	8
5	Основи технічного захисту інформації в ІС.	8
6	Перспективні напрями розвитку технічного комплексу ЗІ в розподілених обчислювальних середовищах (РОС).	8

7	Випробування системи технічного захисту інформації та його атестація	8
8	Особливості проектування ТЗІ для АС різних класів. Оцінка ефективності.	8
9	Технічне завдання на створення ТЗІ в АС	8
	Всього	68

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. Назвіть методи підвищення енергетичної та структурної таємності системи передавання інформації.
2. Дайте визначення поняття технічного захисту інформації
3. Які вам відомі підходи до класифікації загроз безпеці інформації?
4. Наведіть класифікаційну структуру каналів несанкціонованого отримання інформації.
5. Дайте визначення поняттю "Технічний канал витоку інформації". Назвіть основні види технічних каналів.
6. Дайте класифікацію джерел витоку інформації.
7. Наведіть відомі вам методи і засоби контролю акустичної інформації.
8. Розкрийте зміст методів контролю інформації технічними засобами в каналах телефонного зв'язку.
9. Охарактеризуйте основні способи запобігання витоку інформації по технічних каналах. Охарактеризуйте способи захисту інформації в каналах зв'язку.
10. Сформулюйте основні концептуальні положення теорії захисту інформації.
11. Як впливають показники інформації, що захищається, на структуру і
12. Підходи до проектування технічної системи захисту інформації?

13. Розкрити критерій вибору засобів і методів захисту.
14. Розкрити задачу мінімізації вартості та ефективності забезпечення систем захисту об’єкта.
15. Розкрити та пояснити заходи, які виконуються при створенні ТЗІ.
16. Програмні закладки та їх складові. Класифікація програмних закладок.
17. Які основні характеристики телекомунікаційної системи як об'єкта захисту.
18. Розкрийте поняття загрози інформаційної безпеки. Які основні напрями захисту інформації?
19. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені.
20. Класифікація загроз інформаційної безпеки за характером впливу
21. Класифікація загроз інформаційної безпеки за розміщенням їх джерела. Які основні види загроз безпеки інформаційним технологіям?
22. Основні техногенні передбачувані та непередбачені загрози інформаційній системи
23. Яку систему складають дестабілізуючі чинники відповідно до технології і функціонування інформації?
24. Привести структуру каналу витоку інформації та дати характеристику середовищу передачі інформації.
25. Якими видами можуть бути представлені природні канали витоку ?
26. Дайте характеристику каналам витоку інформації, які створені закладними пристроями? Які основні тенденції та шляхи розвитку закладних пистроїв?
27. Які основні методи захисту від витоку інформації з обмеженим доступом шляхом прослуховування?
28. Як залежно від типу створюваного електромагнітного поля розрізняють види екранування?
29. Які методи забезпечують зниження потужності випромінювань і наведень?
30. Які основні методи захисту інформації від НСД в автоматизованих системах?
31. Дайте характеристику основним та допоміжним технічним засобам та системам.
32. Розкрийте поняття зони 1, зони 2 та контрольованої зони.
33. Як класифікуються ТКВІ за фізичними ефектами, процесами? Як класифікуються ТКВІ за носієм, що утворюється джерелом небезпечного сигналу?
34. Як класифікуються ТКВІ за способом перехоплення інформації засобами розвідки противника?
35. Дайте характеристику технічним каналам витоку інформації через допоміжні технічні засоби і системи та сторонні провідники.
36. Дайте характеристику електричним каналам витоку інформації, які виникають в результаті просочування небезпечних сигналів в ланцюги електроживлення.
37. Дайте характеристику електричним каналам витоку інформації, які виникають в результаті просочування небезпечних сигналів в ланцюги заземлення.
38. Дайте характеристику параметричним каналам витоку інформації, що обробляється в основних технічних засобах і системах.
39. Дайте характеристику акустичним та акустовібраційним каналам витоку мовної інформації.
40. Дайте характеристику акустоелектричним та акустооптичним каналам витоку мовної інформації.
41. Дайте характеристику параметричним каналам витоку мовної інформації.
42. Умови обробки інформації в системі.

43. Порядок розроблення та оформлення програм і методик випробувань Що наводять у розділі “Вимоги щодо забезпечення охорони державної таємниці».
44. Атестація комплексів ТЗІ.
45. Основні етапи атестації комплексу ТЗІ.
46. Зміст другого етапу створення комплексу ТЗІ “Розроблення та впровадження заходів із захисту інформації” на ОІД.
47. 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. 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.
2. 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
3. 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
4. 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
5. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
6. 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.

7. 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.