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

МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

підготовки бакалавра

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2023

Силабус навчальної дисципліни «Методи та засоби технічного захисту інформації**»** підготовки бакалаврів галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації за освітньою програмою Кібербезпека та захист інформації

Розробник: доцент, кандидат технічних наук Багнюк Наталія Володимирівна

Погоджено
Гарант освітньо-професійної програми:

Глинчук Л.Я.

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

протокол №2_ від 28 листопада 2023 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>Денна форма навчання</td><td rowspan="3">12 Інформаційні технології

125 Кібербезпека та захист інформації
Кібербезпека та захист інформації</td><td>Нормативна</td></tr>
<tr><td rowspan="2">Кількість годин / кредитів
120 / 4</td><td>Рік навчання 4
Семестр 7</td></tr>
<tr><td>Лекції 48 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Лабораторні роботи 60 год.</td></tr>
<tr><td rowspan="2">Перший (бакалаврський)</td><td>Самостійна робота 4 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова навчання</td><td>Форма контролю: екзамен</td></tr>
<tr><td colspan="2"></td><td>українська</td></tr>
</table>

ІІ. Інформація про викладачів

ПІП	Багнюк Наталія Володимирівна
Науковий ступінь	кандидат технічних наук
Вчене звання	доцент
Посада	доцент кафедри комп’ютерних наук та кібербезпеки
Контактна інформація	(095) 55 25 009, bahniuk.nataliia@vnu.edu.ua
Дні занять	за розкладом http://94.130.69.82/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація курсу

Курс «Методи та засоби технічного захисту інформації» є обов’язковим освітнім компонентом освітньо-професійної програми «Кібербезпека та захист інформації» бакалаврського рівня. Дисципліна спрямована на підвищення рівня обізнаності щодо нормативно-правової бази у сфері ТЗІ та технічних засобів захисту інформації. У курсі викладені основні положення та нормативні акти для ТЗІ, класифікація каналів витоку інформації, методи та засоби захисту від витоку; фізичні та апаратні засоби захисту інформації.

З метою кращого засвоєння навчального матеріалу дисципліни студенти повинні до його початку опанувати такі предмети: сучасне програмне забезпечення та хмарні технології, новітні інформаційні технології для аналізу і обробки даних, теорія інформації та кодування, архітектура комп'ютерних систем та схемотехніка.

Найбільш яскраво виражені міждисциплінарні зв’язки з діагностикою шкідливого програмного забезпечення та захистом інформації в операційних системах.

2. Мета і завдання освітнього компонента

Мета дисципліни полягає в освоєнні принципів побудови ТЗІ в комп’ютерних системах, а також формування умінь використовувати на практиці набуті знання для аналізу

захищеності сучасного обладнання та програмного забезпечення, проектування та експлуатації ефективної системи захисту інформації від несанкціонованого доступу. Формування професійних навиків від користування необхідною нормативно-правовою базою до вибору та експлуатації технічних пристроїв для захисту інформації на відповідних ОІД.

Завдання: основними завданнями вивчення дисципліни «Кібербезпека та захист інформації» є надання студентам знань про системи технічного захисту інформації, поняття з використання систем технічного захисту інформації, канали витоку інформації, застосування систем технічного захисту інформації.

3. Результати навчання та компетентності

Вивчення навчальної дисципліни «Кібербезпека та захист інформації» сприяє формуванню та розвитку у здобувачів таких загальних та спеціальних компетентностей:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Очікувані програмні результати навчання, які забезпечуються зокрема освітнім компонентом «Технічний захист інформації» у комплексі з іншими компонентами освітньої програми:

ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних- засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

4. Структура освітнього компонента

Назви змістових модулів і тем	Кількість годин					Форма контролю / Бали
	Усього	у тому числі				
		Лекції	Лабораторні заняття	Консультації	Самостійна робота	
Змістовий модуль 1						

1. Тема 1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням. Положення про державну експертизу в сфері технічного захисту інформації.	12	4	6	2		Зах. ЛР
Тема 2. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	12	4	6	2		Зах. ЛР
Тема 3. Порядок проведення перед проектних досліджень на об'єкті інформаційної діяльності.	10	4	6			Зах. ЛР
Тема 4. Методи за засоби захисту від витоку інформації.	11	4	6		1	Зах. ЛР
Тема 5. Поняття інженерно-технічного захисту. Фізичні засоби захисту: охоронні системи, охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації.	13	6	6		1	Зах. ЛР
Разом за змістовим модулем 1	**58**	**22**	**30**	**4**	**2**	**20 б.**
Змістовий модуль 2						
Тема 6. Апаратні засоби захисту. Ключові елементи, персональні кодові карти, персональний ідентифікатор, пристрої розпізнавання голосу користувача чи форми його пальців.	12	4	6	2		Зах. ЛР
Тема 7. 9. Класифікація закладних пристроїв, їх основні характеристики та застосування. Способи та засоби боротьби.	14	6	6	2		Зах. ЛР
Тема 8. 10. ТЗІ на мережевому рівні.	11	4	6		1	Зах. ЛР
Тема 9. 11. Система технічного захисту інформації в Україні: стан та напрями розвитку.	13	6	6		1	Зах. ЛР
Тема 10. Огляд засобів для технічного захисту на ринку України та дозвіл користування ними.	12	6	6			Зах. ЛР
Разом за змістовим модулем 2	**62**	**26**	**30**	**4**	**2**	**20 б.**
Всього годин / Балів	**120**	**48**	**60**	**8**	**4**	**40 б.**

Види підсумкових робіт	**Бали**
Модульна контрольна робота за ЗМ1	30 б.
Модульна контрольна робота за ЗМ2	30б.
Всього балів за МКР	**60 б.**

5. Завдання для самостійного опрацювання

№ п/п	Тематика	К-сть годин
1	Характеристика носіїв інформації та їх види.	6
2	Апаратні засоби захисту інформації та класифікація технічних каналів витоку інформації.	6
3	Нормативні документи у сфері ТЗІ.	6
4	Організаційні заходи ТЗІ.	6
5	Основні об'єкти захисту інформації.	8
6	Основні принципи і концептуальні засади організації забезпечення ТЗІ в Україні.	6
7	Пасивні способи захисту інформації	6
Разом		**44**

IV. Політика оцінювання

Політика оцінювання та організація контрольних заходів здійснюється згідно з Положенням про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки https://bit.ly/3RXsLvA .

Оцінювання навчальних досягнень з Комп'ютерних мереж здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань, самостійне опрацювання теоретичного матеріалу) та підсумковий модульний контроль (письмові модульні контрольні роботи). Максимальна кількість балів, яку може накопичити здобувач під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за модульні контрольні роботи (МКР). Максимальна кількість балів, яку може накопичити здобувач під час модульного контролю за семестр, складає 60 балів. Модульні контрольні роботи складаються з тестів по темах. Упродовж семестру, після завершення відповідних тем (модулів), проводяться М1, М2 модульні контрольні роботи у тестовій формі.

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 разі 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.

1. Політика викладача щодо здобувача

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих морально-етичних 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 без поважних причин; користування мобільним телефоном або іншими мобільними пристроями під час заняття не з навчальною метою, зокрема розмови, переписка, ігри та інші розваги; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу. У випадку запровадження дистанційної форми навчання, що може бути пов'язано із карантином, надзвичайними ситуаціями, воєнним станом і т. ін., заняття проводитимуться в режимі відео конференції Zoom та / або з

використанням платформи Moodle https://moodle-cs.vnu.edu.ua/. Матеріал пропущених занять здобувач опрацьовує самостійно, звітує про виконання викладачу в індивідуальному порядку. Пропущені заняття не звільняють студента від вчасного виконання модульних контрольних робіт разом із групою.

Перезарахування окремих змістових модулів, модульних контрольних заходів в межах освітнього компонента регламентується Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки https://bit.ly/3Bdq6qP .

2. 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 https://bit.ly/3BFUETR .

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.

3. 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 завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

V. Підсумковий контроль

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 разі 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. Оцінка за семестр у випадку складання іспиту є сумою балів поточного контролю та балів, отриманих під час іспиту.

Перелік питань до екзамену

1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням.
2. Положення про державну експертизу в сфері технічного захисту інформації.
3. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
4. Порядок проведення перед проектних досліджень на об'єкті інформаційної діяльності.

5. Рекомендації щодо розроблення технічного завдання на виконання робіт із створення комплексу захисту на об’єкті інформаційної діяльності.

6. Система технічного захисту інформації в Україні: стан та напрями розвитку.

7. Перехоплення даних.

8. Класифікація каналів витоку інформації.

9. Технічні канали витоку інформації.

10. Методи за засоби захисту від витоку інформації.

11. Поняття інженерно-технічного захисту.

12. Фізичні засоби захисту: охоронні системи.

13. Фізичні засоби захисту: охоронне телебачення.

14. Фізичні засоби захисту: охоронне освітлення.

15. Фізичні засоби захисту: засоби охоронної сигналізації.

16. Апаратні засоби захисту.

17. Ключові елементи: ключові дискети, USB- та LPT-ключі.

18. Персональні кодові карти.

19. Персональний ідентифікатор.

20. Пристрої розпізнавання голосу користувача чи форми його пальців.

21. Класифікація закладних пристроїв.

22. Основні характеристики закладних пристроїв.

23. Застосування закладних пристроїв.

24. Пристрої для захисту інформації у мережах.

25. Класи безпеки інформаційних систем.

26. Загрози безпеці інформації.

27. Основні поняття та класифікація загроз.

28. Порушники інформаційної безпеки, їх класифікація.

29. Модель поводження потенційного порушника.

30. Критерії оцінювання безпеки інформаційних технологій.

31. Моделі управління доступом.

32. Моніторинг ринку України на наявність приладів для захисту інформації.

33. Апаратні засоби захисту в мережах.

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

1. Комплексні системи захисту інформації [Текст]: навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.]; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018. - 118 с. - Бібліогр.: с. 116-117.
2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В.Захист інформації в автоматизованих системах управління: посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
3. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
4. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.
5. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
6. Толюпа С.В., Дружинін В.А., Бурячок В.Л., Наконечний В.С., Лазаренко С.В. Електроматеріали. Пасивні елементи засобів радіозв’язку та захисту інформації. Навчальний посібник. – К.: ДУТ, 2015. – 193 с
7. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
8. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. –Житомир: ЖНАЕУ, 2016. – 636 с.
9. Барило Г.І., Вісьтак М.В., Готра З.Ю., Лесінський В.В., Політанський Л.Ф. Електронні елементи та пристрої систем безпеки й охорони: Навчальний посібник .- За ред. Готри З.Ю. – Чернівці: Рута, 2017. 216 с. ISBN 978-966-423-419-8.

Додаткова

1. Закон України «Про інформацію»
2. Закон України «Про державну таємницю»
3. Положення про технічний захист інформації в Україні УП №1229/99 від 27.09.99.
4. Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.97 р., № 1126.
5. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.
6. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

7. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
8. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення 12. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
9. НБУ № 243 04.07.07 Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи.