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

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ

Підготовки першого (бакалаврського) рівня вищої освіти
Спеціальності 125 Кібербезпека та захист інформації
Освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2025

Силабус нормативного освітнього компонента “Управління інформаційною та кібербезпекою” підготовки бакалаврів, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації

Розробники:
Чернящук Наталія Леонідівна, доктор педагогічних наук, професор, професор кафедри комп’ютерних наук та кібербезпеки

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

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

протокол № 2 від 17.09.2025 р.

Завідувач кафедри: Гришанович Т. О.

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="6">Галузь знань
12 Інформаційні технології,
спеціальність
125 Кібербезпека та захист інформації,
освітньо-професійна програма
Кібербезпека та захист інформації
освітній рівень бакалавр.</td><td>Рік підготовки 4</td></tr>
<tr><td rowspan="3">Кількість
Годин/кредитів
120/4</td><td>Семестр 7</td></tr>
<tr><td>Лекції 48 год.</td></tr>
<tr><td>Лабораторні 60 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Самостійна робота 4 год.</td></tr>
<tr><td>Консультації 8 год.
Форма контролю: екзамен</td></tr>
<tr><td colspan="3">Мова навчання – Українська</td></tr>
</table>

ІІ Інформація про викладача

ПІП: Чернящук Наталія Леонідівна;
Науковий ступінь: доктор педагогічних наук;
Вчене звання: професор;
Посада: професор кафедри комп'ютерних наук та кібербезпеки;
Контактна інформація: Cherniashchuk.Nataliia@vnu.edu.ua
Дні занять: http://94.130.69.82/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

Анотація освітнього компонента. Силабус освітнього компонента «Управління інформаційною та кібербезпекою» складено відповідно до освітньо-професійної програми «Кібербезпека та захист інформації» першого рівня вищої освіти галузі знань 12 Інформаційні технології, за спеціальністю 125 Кібербезпека та захист інформації. Освітній компонент «Управління інформаційною та кібербезпекою» належить до переліку нормативних навчальних дисциплін, забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, вмінь та формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації; формування у майбутніх фахівців здатності діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

Пререквізити: базові знання з інформаційних технологій і комп'ютерних мереж, основи кібербезпеки та криптографії, базові навички оцінки ризиків і знання нормативних вимог у сфері захисту інформації.

Постреквізити: здобуття навичок управління інформаційною безпекою організацій, оцінки та мінімізації інформаційних ризиків, розробки політик безпеки, планування заходів захисту даних та впровадження стандартів інформаційної безпеки.

Мета і завдання освітнього компонента: є систематизація інформації щодо розроблення, впровадження та експлуатації систем захисту інформації на об'єктах інформаційної діяльності; формування у майбутніх фахівців здатності діяти на основі

законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Завдання освітнього компонента: надати знання про сучасні загрози та вразливості інформаційних систем; ознайомити з методами управління ризиками та контролю інформаційної безпеки; розвинути навички розробки та впровадження політик і процедур інформаційної безпеки; сформувати компетенції використання нормативних документів та стандартів (ISO/IEC 27001, NIST, GDPR) у практичній діяльності; розвинути аналітичне та критичне мислення для прийняття рішень щодо захисту інформаційних активів організації.

Компетентності. Програмні результати навчання. Soft skills.

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

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

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

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

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. 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.)

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною кібербезпекою.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості загрози інформаційному простору інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

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

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги , практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН13. 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.

РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН17. 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.

РН21. 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.

Аналітичне мислення – здатність оцінювати ризики, виявляти вразливості та приймати обґрунтовані рішення щодо безпеки.

Комунікаційні навички – уміння ефективно пояснювати політики безпеки, навчати персонал та взаємодіяти з колегами різних відділів.

Проблемне мислення – здатність швидко реагувати на інциденти та знаходити оптимальні рішення у стресових ситуаціях.

Організаційні навички – планування та координація заходів із захисту інформації, управління проєктами.

Етична відповідальність – дотримання конфіденційності, правил етики та законодавчих вимог у сфері інформаційної безпеки.

Структура освітнього компонента:

Програма навчальної дисципліни складається з таких **змістових модулів**:

1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки .Управління кіберінцидентами.

2. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту).

Назви змістових модулів і тем	**Кількість годин**					**Форма контролю / бали**
	Усього	**у тому числі**				
		Лек.	**Лаб.**	**Сам. роб.**	**Конс.**	
1. Змістовий модуль 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки. Управління кіберінцидентами.						Тестовий контроль знань / 15
Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки. Управління кіберінцидентами.	10	3	4		1	Звіт по лаб. роботі /5

Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки	6	3	4			Звіт по лаб. роботі /5
Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки	8	3	4		1	Звіт по лаб. роботі /5
Тема 4. Роботи спеціалізованих міжнародних організацій та об'єднань в галузі інформаційної безпеки. Управління ризиками в інформаційній та кібербезпеці.	10	3	4		1	Звіт по лаб. роботі /5
Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем	12	4	4	1	1	Звіт по лаб. роботі /5
Тема 6. Організаційне забезпечення інформаційної безпеки на Державному рівні: практика США	6	4	5	1		Звіт по лаб. роботі /5
Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України	6	4	5			Звіт по лаб. роботі /5
Разом за змістовим модулем 1	58	24	30	2	4	50
Змістовий модуль 2. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту).						Тестовий контроль знань / 15
Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту)	6	3	4		1	Звіт по лаб. роботі /4
Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту). Характеристика кіберзлочинності. Стан кіберзлочинності в Україні. Боротьба із кіберзлочинами.	6	3	4	1	1	Звіт по лаб. роботі /4
Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки	6	3	4	1	1	Звіт по лаб. роботі /4
Тема 11. Зміст деталізованої політики безпеки	10	3	4			Звіт по лаб. роботі /4
Тема 12. Департамент інформаційної безпеки і робота з персоналом	8	3	4			Звіт по лаб. роботі /4
Тема 13. Організація реагування на надзвичайні ситуації (інциденти)	10	3	4		1	Звіт по лаб. роботі /5
Тема 14. Аудит стану інформаційної безпеки на підприємстві. Надання послуг у сфері інформаційної безпеки (страхування)	8	3	4			Звіт по лаб. роботі /5
Тема 15. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей.	8	3	2			Звіт по лаб. роботі /5
Разом за змістовим модулем 2	62	24	30	2	4	50
Всього годин/Балів	**120**	**48**	**60**	**4**	**8**	120 год. / 100 балів

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	**1**
2	Опрацювання лекційного матеріалу	**1**
3	Оформлення результатів лабораторних робіт	**1**
4	Систематизація здобутих знань перед екзаменом	**0,5**
5	Робота з літературою в бібліотеці	**0,5**
	Разом	**4**

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу зобов'язані дотримуватись вимог чинного законодавства України, Статуту та Правил внутрішнього розпорядку Волинського національного університету імені Лесі Українки, а також загальноприйнятих норм академічної етики, корпоративної культури та взаємоповаги. Під час занять з ОК «Управління інформаційною безпекою» підтримується атмосфера співпраці, відкритості, відповідальності й толерантності. Очікується активна участь студентів у лекційних і лабораторних заняттях, своєчасне виконання індивідуальних та групових завдань, дотримання графіка навчання та вимог до оформлення робіт. Недопустимими є запізнення, використання мобільних пристроїв не за навчальним призначенням, плагіат, списування, підміна особи та будь-які прояви порушення академічної доброчесності. Усі лабораторні, самостійні й підсумкові завдання виконуються із використанням засобів дистанційного курсу дисципліни в системі Moodle. Викладач гарантує прозорість та об'єктивність оцінювання, надання зворотного зв'язку, створення комфортних умов для засвоєння матеріалу й розвитку професійних і комунікаційних компетентностей здобувачів освіти.

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), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Політика дедлайнів та перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній 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».

Можливість отримати додаткові бали.

Здобувачі освіти можуть отримати додаткові бали за активну участь у навчальному процесі, своєчасне та якісне виконання практичних і самостійних завдань, ініціативність під час обговорень, а також за виконання завдань підвищеної складності. Додаткові бали можуть нараховуватися за: участь у науково-дослідній діяльності, конференціях, олімпіадах або конкурсах з питань інформаційної безпеки; розробку власних мініпроєктів або практичних рішень з кіберзахисту; створення навчальних матеріалів, презентацій чи довідників для одногрупників; відвідування всіх занять без пропусків та активну участь у лекціях і практичних заняттях. Нарахування додаткових балів здійснюється в межах, визначених критеріями оцінювання, і не може перевищувати граничне значення, передбачене системою оцінювання дисципліни (70 балів).

V. Підсумковий контроль

Оцінювання здійснюється за 100-бальною шкалою і включає поточний контроль (активність на заняттях, лабораторні роботи) – до 70 балів, та підсумковий контроль (тести) – 30 балів. Для допуску до підсумкового контролю студент повинен набрати не менше 35 балів під час поточного оцінювання та виконати всі лабораторні роботи. Студенти, які набрали 75 і більше балів за семестр і виконали всі завдання, можуть отримати підсумкову оцінку без складання іспиту.

Питання, які виносяться на залік під час ліквідації академічної заборгованості.

1. Загальні поняття щодо інформаційної безпеки
2. Основні поняття та визначення дисципліни
3. Основні нормативно-правові документи України у сфері ІБ
4. Основні ненавмисні штучні загрози
5. Основные навмисні штучні загрози
6. Класифікація загроз безпеки
7. Опис моделі гіпотетичного порушника
8. Види інформації, що захищається у сфері управління
9. Контроль якості захисту інформації
10. Класифікаційна політика у сфері інформації
11. Джерела загроз інформаційної безпеки
12. Сертифікація: створення захищеної роботи
13. Відмінності мережі від обчислюваного центру
14. Характеристика ефективних стандартів щодо безпеки
15. Усна форма разповсюдження матеріалів із стандартів по ІБ
16. Визначення вразливих місць персонального комп’ютера
17. Мережевий захист ПК
18. Планування безпечної роботи на ПК
19. Принципи інженерно-технічного захисту інформації
20. Методи захисту інформації технічними засобами
21. Канали витоку інформації
22. Засоби забезпечення ІБ в комп’ютерних системах
23. Стратегії комплексного захисту інформації

VI. Шкала оцінювання

Шкала оцінювання (національна та ECTS)

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

0–59	Незадовільно	Fx	Необхідне перескладання

VI. Рекомендована література та інтернет-ресурси

1. Управління інформаційною безпекою: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Чернящук, Луцьк: ЛНТУ, 2022. 120 с.

2. Управління інформаційною безпекою: Методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Чернящук. Луцьк: ЛНТУ, 2022. 34 с.

3. Управління інформаційною безпекою: Методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Чернящук. Луцьк: ЛНТУ, 2022. 24 с.

Додаткова література:

1. Nataliia Chernyaschuk Oleksandr Bezkrevnyi, Leonid Kupershtein.The analysis handwarefor recording image and video and processing on fpga. The International Society for Optical Engineering Vol. 11176 (1): 11176-201, 11 pag. The International Society for Optical Engineering Vol. 11176 (1): 11176-201, 5 pag. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/browse/volume-number/11000-NOW/11100-11199.2019 DOI 10.1117/12.2536310 SCOPUS

2. Vasyl Melnyk, Olena Kuzmych, Nataliia Bahniuk, Nataliia Cherniashchuk, Liudmyla Hlynchuk, Oksana Mekush. Effective Big Data Analysis Based on Sockets Application to Biomedical Data Processing - Conference Proceedings, 2021 11th International Conference on Advanced Computer Information Technologies, 15-17 September 2021, page 19

3. Kuzmych, O., Cherniashchuk, N., Lishchyna, N., Mekush, O., Gumenyuk, P. Mobile Robot Motion Stability and Optimal Chassi Construction 2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021. Proceedingsc. 141-146

4. Мельник, В., Каганюк О., Козленко, М., Чернящук, Н., & Щерблюк, А. (2020). Залежність інтенсивності обробки даних в кластері від продуктивності сокетів без врахування гетерогенності. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО, (40), 128-139. https://doi.org/10.36910/6775-2524-0560-2020-40-20

5. Костючко С., Чернящук Н., Поліщук М., Кирилюк Л., Сахнюк А. Застосування систем виявлення вторгнень. Технічні вісті. 1(51), 2 (52). Львів, 2020. С. 81-82.

6. Костючко С., Кирилюк Л., Чернящук Н., Бортник К., Гринюк С.. Бездротова точка доступу з багаторівневим алгоритмом захисту даних (Англійською мовою). КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО, (42), Луцьк, 2021. С. 128-139. https://doi.org/10.36910/6775-2524-0560-2021-42.

7. Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л. Основні загрози безпеці інформаційних систем. // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк: Видавництво ЛНТУ. Вип. 40. 2020. С. 137-142.

8. Глинчук Л.Я., Яцюк С.М., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л. Аналіз вимог та методологія підбору тем для вивчення основ криптографічного захисту інформації. // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк: Видавництво ЛНТУ. Вип. 40. 2020. С. 16-22.