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

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Підготовки першого (бакалаврського) рівня вищої освіти
Спеціальності F5 Кібербезпека та захист інформації
Освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2025

Силабус нормативного освітнього компонента “Організаційне забезпечення захисту інформації” підготовки бакалаврів, галузі знань F Інформаційні технології, спеціальності F5 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
F Інформаційні технології,
спеціальність
F5 Кібербезпека та захист інформації,
освітньо-професійна програма
Кібербезпека та захист інформації
освітній рівень бакалавр.</td><td>Рік підготовки 1</td></tr>
<tr><td rowspan="3">Кількість
Годин/кредитів
120/4</td><td>Семестр 2</td></tr>
<tr><td>Лекції 20 год.</td></tr>
<tr><td>Лабораторні 34 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Самостійна робота 58 год.</td></tr>
<tr><td>Консультації 8 год.
Форма контролю: залік</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. Освітній компонент «Організація забезпечення захисту інформації» спрямований на формування у здобувачів освіти системного розуміння принципів, методів та засобів організації інформаційної безпеки в сучасних інформаційно-комунікаційних системах. Дисципліна розкриває концептуальні засади створення, впровадження та підтримання систем управління інформаційною безпекою (СУІБ) відповідно до міжнародних стандартів ISO/IEC 27000, національних нормативно-правових актів та кращих практик галузі. У межах курсу розглядаються питання класифікації інформаційних ресурсів, визначення рівнів захисту, управління ризиками, розроблення політики безпеки, організаційних структур і ролей у сфері ІБ, реагування на інциденти, аудиту та підвищення ефективності системи захисту. Вивчення дисципліни забезпечує здобуття компетентностей у сфері планування, організації, контролю та вдосконалення заходів із забезпечення конфіденційності, цілісності та доступності інформації. Особлива увага приділяється людському фактору, питанням управління доступом, кібергігієни та корпоративної культури безпеки. Результатом опанування курсу є формування здатності проєктувати, впроваджувати та підтримувати організаційну модель захисту інформації на рівні підприємства, установи чи інформаційної системи.

Пререквізити: основи інформаційної безпеки, криптографічний захист інформації, правові засади ІБ.

Постреквізити: аудит інформаційної безпеки, управління ризиками, менеджмент кібербезпеки, реагування на інциденти інформаційної безпеки.

Мета і завдання освітнього компонента: формування у здобувачів освіти знань, умінь і навичок з організації системи захисту інформації, управління процесами інформаційної безпеки та забезпечення ефективного функціонування систем захисту відповідно до міжнародних і національних стандартів. Завдання освітнього компонента: ознайомити здобувачів із принципами та моделями організації захисту інформації; сформувати розуміння структури та функцій систем управління інформаційною безпекою; навчити розробляти політики, процедури й регламенти безпеки; розвинути навички оцінювання ризиків та планування заходів із їх мінімізації; підготувати до практичного застосування методів контролю, аудиту та реагування на інциденти інформаційної безпеки.

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.

ЗК5. 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.

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.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

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.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

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.

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.

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.

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:

Назви змістових модулів і тем	Кількість годин					Форма контролю / бали
	Усього	у тому числі				
		Лек.	Лаб.	Конс.	Сам. Роб.	
1. Змістовий модуль 1.						Тестовий контроль знань / 15
Тема 1. Система національного законодавства України у сфері кібербезпеки.	9	1	2		4	Звіт по лаб. роботі /5
Тема 2. Система міжнародних законодавства та стандартів у сфері інформаційної/кібербезпеки.	9	2	2		4	Звіт по лаб. роботі /5
Тема 3. Системи управління інформаційною безпекою. Основні принципи побудови СУІБ.	9	2	2	1	4	Звіт по лаб. роботі /5
Тема 4. Основи управління інформаційними ризиками.	9	2	2	1	4	Звіт по лаб. роботі /5
Тема 5. Напрямки побудови СУІБ. Політика ІБ організації. Фізична безпека організації та устаткування. Управління комп'ютерами та мережами. Управління доступом. Вимоги до інформаційних систем.	8	1	3	1	4	Звіт по лаб. роботі /5
Тема 6. Управління інцидентами в СУІБ. Питання Безперервності функціонування	8	1	3	1	4	Звіт по лаб. роботі /5

організації.						
Тема 7. Внутрішній аудит СУІБ.	8	1	3		5	Звіт по лаб. роботі /5
Разом за змістовим модулем 1	60	10	17	4	29	50
Змістовий модуль 2.						Тестовий контроль знань / 15
Тема 8. Методика впровадження СУІБ.	8	1	2		4	Звіт по лаб. роботі /4
Тема 9. Розробка документа політики інформаційної безпеки та цілей СУІБ. Управління інформаційними активами.	8	1	2	1	4	Звіт по лаб. роботі /4
Тема 10. Впровадження системи управління інформаційними ризиками.	8	1	2	1	4	Звіт по лаб. роботі /4
Тема 11. Розробка та обґрунтування заходів з обробки та зниженню інформаційних ризиків.	8	1	2	1	4	Звіт по лаб. роботі /4
Тема 12. Структура документації СУІБ та порядок її розробки. Розробка управлінських процедур.	7	2	2	1	4	Звіт по лаб. роботі /4
Тема 13. Розробка плану безперервності функціонування організації.	7	2	2		3	Звіт по лаб. роботі /5
Тема 14. Розробка процедур реагування на надзвичайні ситуації.	7	1	2		3	Звіт по лаб. роботі /5
Тема 15. Розробка процедур переходу на аварійний режим. Введення в дію СУІБ.	7	1	3		3	Звіт по лаб. роботі /5
Разом за змістовим модулем 2	60	10	17	4	29	50
Всього годин/Балів	**120**	**20**	**34**	**8**	**58**	120 год. / 100 балів

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	**12**
2	Опрацювання лекційного матеріалу	**11**
3	Оформлення результатів лабораторних робіт	**11**
4	Систематизація здобутих знань перед екзаменом	**12**
5	Робота з літературою в бібліотеці	**12**
	Разом	**58**

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 «Організація забезпечення захисту інформації» 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. Поняття інформаційної безпеки та її основні принципи.
2. Основні загрози та вразливості інформаційних систем.
3. Конфіденційність, цілісність і доступність інформації (CIA-трійка).
4. Законодавче та нормативне забезпечення інформаційної безпеки в Україні.
5. Міжнародні стандарти у сфері ІБ (ISO/IEC 27001, ISO/IEC 27002).
6. Основні завдання організації захисту інформації.
7. Мета та завдання систем управління інформаційною безпекою (СУІБ).
8. Політика інформаційної безпеки: структура та зміст.
9. Процедури та регламенти в системі управління ІБ.

10. Управління доступом до інформаційних ресурсів: принципи та моделі.
11. Методи автентифікації та авторизації користувачів.
12. Роль ролей і груп у контролі доступу.
13. Методи оцінювання ризиків інформаційної безпеки.
14. Організаційні та технічні заходи управління ризиками.
15. Класифікація інформаційних ресурсів та визначення рівнів захисту.
16. Організаційна структура СУІБ: ролі та відповідальність.
17. Планування і впровадження заходів інформаційної безпеки.
18. Моніторинг інформаційних систем та журналювання подій.
19. Системи виявлення та реагування на інциденти (IDS/IPS, SIEM).
20. Реагування на інциденти: етапи, документування та відновлення.
21. Резервне копіювання та відновлення даних: типи та стратегії.
22. Контроль конфігурацій і управління змінами в системах безпеки.
23. Фізичний захист інформаційних систем та контроль доступу до об’єктів.
24. Захист персональних даних та дотримання законодавчих вимог (GDPR, Закон України «Про захист персональних даних»).
25. Аудит інформаційної безпеки: цілі, методи, основні процедури.
26. Метрики та показники ефективності заходів інформаційної безпеки.
27. Практичні приклади реалізації організаційних заходів безпеки у різних організаціях.
28. Побудова комплексного плану захисту інформації для організації.
29. Основні помилки при організації захисту інформації та способи їх уникнення.
30. Сучасні тенденції та перспективи розвитку організації інформаційної безпеки.

VI. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
0–59	Незараховано (необхідне перескладання)

VI. Рекомендована література та інтернет-ресурси

1. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ: ДП «УкрНДНЦ», 2023.
2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. – Geneva: ISO, 2022.
3. Козленко, В. О., Кузнецов, О. О. Організація та управління інформаційною безпекою. – Київ: КНУ ім. Т. Шевченка, 2022.
4. Баранов, О. А., Семенюк, М. В. Інформаційна безпека: організаційно-технічні аспекти. – Харків: ХНУРЕ, 2021.
5. Черняк, Л. І. Системи захисту інформації: концепції, технології, управління. – Київ: НАУ, 2020.
6. Бойко, А. П. Організаційно-правові основи забезпечення інформаційної безпеки. – Львів: ЛНУ, 2021.
7. National Institute of Standards and Technology (NIST). SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg: NIST, 2020.

8. Степаненко, І. С. Менеджмент інформаційної безпеки: сучасні підходи. – Одеса: ОНАХТ, 2022.
9. Шевченко, П. В. Політика інформаційної безпеки організацій: розробка та впровадження. – Київ: КПІ ім. І. Сікорського, 2023.
10. European Union Agency for Cybersecurity (ENISA). Cybersecurity Guidelines and Good Practices. – Luxembourg: ENISA, 2023.
11. Воронін, В. І. Захист інформації в комп'ютерних системах і мережах. – Київ: Видавництво "Кондор", 2020.
12. ISO/IEC 27035-1:2023. Information security incident management — Part 1: Principles of incident management.– Geneva: ISO, 2023.
13. Мандзяк, О. М. Організаційні аспекти кіберзахисту підприємств. – Тернопіль: ТНТУ, 2022.
14. Whitman, M. E., Mattord, H. J. Principles of Information Security. – 7th ed. – Boston: Cengage Learning, 2022.
15. Stallings, W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2023.
16. 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.
17. 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.
18. 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.
19. 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.