Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативного освітнього компонента

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	01 Освіта/Педагогіка
Спеціальність	014 Середня освіта (Інформатика)
Освітньо-професійна програма	Середня освіта. Інформатика
Форма навчання	Денна
Розробник (викладач)	Гаращенко Володимир Вікторович, старший викладач кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки, фахівець із безпеки.
Контактна інформація	Електронна адреса викладача: harashchenko.volodymyr@vnu.edu.ua
Семестр, курс	8 семестр, IV курс
Кількість годин/кредитів	Загальний обсяг: 4 кредити / 120 годин. Аудиторних годин: 48; з них: лекцій – 24 год., лабораторних – 24 год., самостійної роботи – 64 год., консультації – 8 год.
Форма контролю	Залік
Час занять	Тижневих годин: 4 год. Аудиторні заняття проводяться за розкладом: http://94.130.69.82/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація курсу	Силабус нормативного освітнього компонента «Технології захисту інформації» складено відповідно до освітньо-професійної програми Середня освіта. Інформатика. Викладання курсу спрямоване на підвищення рівня формування у здобувачів освіти знань та умінь, які дадуть теоретичний і практичний фундамент, необхідний для аналізу та усунення виникаючих загроз при зберіганні, обробленні та передачі інформації.
Пререквізити	«Прикладне програмне забезпечення та хмарні технології», «Програмування», «Бази даних», «Комп'ютерні мережі та інтернет-технології»
Постреквізити	Знання та вміння, набуті в результаті вивчення освітнього компонента, можна використати у професійній діяльності з використанням різного виду захисту інформації.
Мета вивчення освітнього компонента	**Метою** викладання освітнього компонента «Технології захисту інформації» є освоєння студентами необхідних знань та отримання навиків з організації та забезпечення захисту інформації засобами операційних систем, за допомогою відповідного програмного забезпечення та нормативно-правової бази. Основними **завданнями** вивчення ОК «Технології захисту інформації» дати наступні **знання**: про методи захисту інформації; нормативно-правову базу, стандарти безпеки, механізми та політики розмежування прав доступу; основні види шкідливого програмного забезпечення, загрози; тестування на проникнення; методи та засоби

	забезпечення інформаційної безпеки в ОС, мережі; біометричний захист **та вміння**: використовувати методи і засоби захисту в ОС, мережі і т.д.; орієнтуватись у системі нормативно-правових документів захисту інформації; застосовувати розмежування прав, політики доступу та механізми контролю, паролі; використовувати засоби криптографічного захисту. Освітній компонент «Технології захисту інформації» спрямований на формування таких **загальних та спеціальних (фахових - ФК, предметних - ПК) компетентностей**: **ЗК1.** Здатність до абстрактного мислення, аналізу та синтезу, до застосування знань у практичних ситуаціях. **ЗК2.** Знання й розуміння предметної області та професійної діяльності. **ЗК4.** Здатність орієнтуватися в інформаційному просторі, здійснювати пошук, аналіз та обробку інформації з різних джерел, ефективно використовувати цифрові ресурси та технології в освітньому процесі. **ЗК8.** Здатність зберігати та примножувати моральні, культурні, наукові цінності та досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та значення у розвитку суспільства, техніки і технологій. **ФК1.** Здатність застосовувати систематизовані наукові знання в професійній діяльності відповідно до предметної спеціальності. **ПК5.** Володіння технологіями налагодження, обслуговування та експлуатації комп'ютерної мережі; здатність реалізовувати комплекс заходів, спрямованих на забезпечення захищеності інформації, здатність формувати вміння безпечної роботи школярів у комп'ютерній мережі.
Результати навчання	**Опанування змісту освітнього компоненту дозволяє отримати наступні програмні результати навчання:** **РН7**. *Застосовувати* систематизовані наукові знання в професійній діяльності відповідно до предметної спеціальності, *оперувати* базовими категоріями та поняттями предметної області спеціальності. **РН9.** *Застосовувати* сучасні інформаційно-комунікаційні та цифрові технології у професійній діяльності. **РН10.** *Демонструвати* володіння сучасними технологіями пошуку наукової інформації для самоосвіти та застосування її у професійній діяльності. **ПРН6.** *Знати* та *розуміти* етично-правові засади використання інформаційно-комунікаційних технологій; *застосовувати* засоби й методи захисту інформації та безпеки в мережі Інтернет.

Структура освітнього компонента

Назви змістових модулів і тем	Усього (год.)	Лек. (год.)	Лабор. (год.)	Сам. роб. (год.)	Конс. (год.)	Форма контролю/ Бали
Змістовий модуль 1. Основні поняття, нормативно-правова база, захист засобами ОС та антивірусним ПЗ, види шкідливого ПЗ						
Тема 1. Огляд безпеки системи. Захист інформації та його основні завдання. Законодавство України у сфері захисту інформації. Стандарти. Поняття та захист авторського права. Поняття плагіату. Огляд програмного забезпечення призначеного для виявлення плагіату	10	2	2	6		Звіт/3
Тема 2. Захист інформації засобами операційної системи. Аутентифікація. Використання паролів (правила створення і керування) і механізмів контролю за доступом. Поняття батьківського контролю	11	2	2	6	1	Звіт/6
Тема 3. Резервне копіювання та його класифікація. Видалення/відновлення даних. Захист даних. Способи захисту pdf/текстових документів/електронних таблиць	11	2	2	6	1	Звіт/3
Тема 4. Поняття шкідливого програмного забезпечення, його види. Як працює та як проявляється. Соціальна інженерія, небезпека для дітей в мережі Інтернет. Відповідальність за створення, розповсюдження та використання шкідливого ПЗ	11	2	2	6	1	Звіт/3
Тема 5. Огляд методів виявлення шкідливих програм. Класифікація та можливості антивірусного ПЗ. Огляд найпоширенішого ПЗ даного типу. Діагностика ПК	15	4	4	6	1	Звіт/5
Разом за змістовим модулем 1	**58**	**12**	**12**	**30**	**4**	**Звіт/20**
Змістовий модуль 2. Безпека в мережі, технічний, криптографічний та біометричний захист. Виявлення вторгнень та тестування на проникнення						
Тема 6. Основи безпеки інформації в комп'ютерних мережах. Безпека в браузерах. Технології Proxy. Особливості віртуальної приватної мережі (VPN). Фільтр доменних імен (DNSFilter), міжмережевий екран (Firewall). Правила роботи у Wi-Fi. Цифровий слід (digital footprint). Безпека в соціальних мережах –	11	2	2	6	1	Звіт/5

етика поведінки						
Тема 7. Технічний та інженерний захист інформації. Канали витоку інформації. Нормативні документи технічного захисту інформації	11	2	2	6	1	Звіт/3
Тема 8. Криптографічний вид захисту інформації: симетричні та асиметричні алгоритми. Цифровий підпис. Програмне забезпечення для здійснення шифрування інформації	9	2	2	4	1	Звіт/6
Тема 9. Системи виявлення та запобігання вторгнень. SIEM-системи. Тестування на проникнення. Особливості біометричного захисту інформації. Біометричні технології	15	2	4	8	1	Звіт/4
Тема 10. Кібервійна як різновид інформаційних війн. Види та характерні риси. Захист кіберпростору України	12	4	2	6		Звіт/2
Разом за змістовим модулем 2	**62**	**12**	**12**	**34**	**4**	**Звіт/20**
Види підсумкових робіт						Бал
Контрольна робота № 1						15
Контрольна робота № 2						15
Індивідуальна робота студента*						30
Всього годин/ Балів	**120**	**24**	**24**	**64**	**8**	**100**

Індивідуальна робота студента* виставляється за наявності сертифікатів з онлайн-курсів поданих на самостійне опрацювання (8, 8, 8, 2, 2, 2 балів відповідно за курс)

Завдання для самостійного опрацювання

№	Тема
1.	Онлайн-курс «Інформаційна безпека» платформа https://prometheus.org.ua/
2.	Онлайн-курс «Інформаційна гігієна під час війни» платформа https://prometheus.org.ua/
3.	Онлайн-курс «Основи кібербезпеки для представників державних органів» https://state-cyber-edu.org/mc/index.php/usr/login/login
4.	Онлайн-курс «Основи кібергігієни» платформа https://osvita.diia.gov.ua/courses/
5.	Онлайн-курс «Безпека дітей в інтернеті» платформа https://osvita.diia.gov.ua/courses/
6.	Онлайн-курс «Кіберняні» https://osvita.diia.gov.ua/courses/cybernanny
7.	Опрацювання лекційного матеріалу
8.	Підготовка до лабораторних робіт

Політика курсу

Політика щодо оцінювання

Оцінювання знань здобувачів освіти здійснюється згідно **Положення про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки**. Освітній компонент складається з двох змістових модулів та його вивчення передбачає виконання лабораторних робіт. У цьому випадку підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

- виконання лабораторних робіт (максимум 40 балів);
- контрольні роботи та індивідуальна робота студента (максимум 60 балів).

Поточний контроль (100 балів)					**Загальна кількість балів**
Змістовий модуль 1	**Змістовий модуль 2**	**КР 1**	**КР 2**	**ІРС**	
Т 1-5	Т 6-10	Т 1-5	Т 6-10	Т1-10	
20	20	15	15	30	100

Якщо за результатами семестру накопичено не менше 60 балів і здобувач освіти погоджується із цим результатом, то оцінка за семестр може виставлятися у відомість. Якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів на заліку під час ліквідації академічної заборгованості становить – 100. Повторне складання заліку-ліквідації допускається не більше як один раз – комісії, яку створює декан факультету.

Поєднання навчання та досліджень. Здобувачі вищої освіти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, зокрема, написання та опублікування наукових тез та статей з тематики ОК. Здобувачам, які брали участь у роботі конференцій, підготовці наукових публікацій, конкурсах студентських наукових робіт за тематикою ОК й досягли значних результатів, може бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю. При цьому загальна кількість балів, що вноситься до відомості за поточну роботу не перевищуватиме 100 б.

Здобувачу освіти також можуть бути зараховані результати навчання, здобуті у процесі формальної, неформальної та/або інформальної освіти відповідно до «Положення про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки». Визнанню можуть підлягати результати навчання, що відповідають тематиці освітнього компоненту, його окремому розділу, темі (темам) або індивідуальному завданню, які здобувач освіти самостійно набув, вивчаючи освітні ресурси (семінари, інтернет-курси, професійні стажування та ін.) на онлайн-платформах Prometheus (https://prometheus.org.ua), EdEra (https://www.ed-era.com) та інших, і підтвердив відповідними сертифікатами.

Навчальні досягнення здобувачів освіти на лабораторних заняттях оцінюються максимум в 3 або 2,5 бали.

К-ть балів	**Критерії оцінювання навчальних досягнень**
3 бал	Оцінюється відповідь здобувача освіти, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки.
2,5 бали	
2,5 бала	Оцінюється відповідь здобувача освіти, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, послуговується науковою термінологією. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки.
2,0 бали	
2,0 бала	Оцінюється відповідь здобувача освіти, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні

1,0 бала	знання окремих положень. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки.
1,5 бала 0,5 бала	Оцінюється робота здобувача освіти, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання освітнього компонента, не розкриває зміст теоретичних питань і практичних завдань.
0 балів	Оцінюється відповідь здобувача освіти, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

Питання до заліку

у випадку ліквідації академічної заборгованості

1. Захист інформації та його основні завдання.
2. Поняття про інформацію з обмеженим доступом.
3. Структура політики безпеки та її основні частини.
4. Життєвий цикл розробки систем безпеки.
5. Законодавство України у сфері захисту інформації.
6. TCSEC («Оранжева книга») – перший стандарт у галузі оцінки захищеності комп'ютерних систем.
7. Common Criteria («Загальні критерії») – європейський стандарт у галузі оцінки захищеності комп'ютерних систем.
8. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу".
9. Поняття та захист авторського права.
10. Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіату.
11. Захист інформації засобами операційної системи. Використання паролів.
12. Формальні моделі доступу. Дискреційний та мандатний доступ до інформації.
13. Аналіз захищеності сучасних операційних систем.
14. Підсистема захисту в ОС Windows.
15. Аутентифікація/двохфакторна аутентифікація користувача.
16. Технології захисту мобільних телефонів на рівні пристрою.
17. Правила для створення надійного та стійкого паролю. Методи злому паролю. Методи створення стійких паролів.
18. Сервіси для перевірки стійкості паролів, менеджери паролів.
19. Поняття батьківського контролю та його налаштування.
20. Резервне копіювання та його класифікація. Рівні зберігання резервних копій.
21. Особливості видалення/відновлення даних.
22. Способи захисту pdf/текстових документів/електронних таблиць
23. Поняття шкідливого програмного забезпечення, його види. Як працює та як проявляється.
24. Соціальна інженерія, її види та особливості. Фішинг.
25. Небезпека для дітей в мережі Інтернет.
26. Що таке комп'ютерний вірус? Де подивитися бібліотеку вірусів?
27. Що таке троянське зловмисне програмне забезпечення?
28. Що таке шпигунське програмне забезпечення?
29. Що таке вимагацьке програмне забезпечення?
30. Відповідальність за створення, розповсюдження та використання шкідливого ПЗ.
31. Класифікація антивірусного ПЗ. Його особливості та функції.
32. Огляд найпоширенішого антивірусного ПЗ. Приклади.
33. Хмарний чи традиційний антивірус? Плюси та мінуси.
34. Основи безпеки інформації в комп'ютерних мережах.

35. Міжмережеві екрани, їх функції та види.
36. VPN-сервіс, особливості та приклади.
37. Безпека в браузерах. Технології Proxy.
38. Особливості віртуальної приватної мережі (VPN).
39. Фільтр доменних імен (DNSFilter), міжмережевий екран (Firewall).
40. Правила роботи у Wi-Fi.
41. Цифровий слід (digital footprint).
42. Інформаційна безпека в соціальних мережах.
43. Технічний та інженерний захист інформації. Ринок приладів для захисту.
44. Канали витоку інформації.
45. Нормативні документи технічного захисту інформації.
46. Криптографічний вид захисту інформації. Основні методи та можливості.
47. Поняття шифрування файлів, папок, повідомлень.
48. Програмне забезпечення для здійснення шифрування інформації.
49. Системи виявлення та запобігання вторгнень.
50. SIEM-системи, їх функції та особливості.
51. Тестування на проникнення.
52. Основні поняття про біометрію. Біометричні характеристики людини.
53. Біометричні системи та технології.
54. Приклади біометричних систем (ринок цін, зовн. вигляд, функції).
55. Огляд ПЗ для обробки біометричних даних.
56. Кібервійна як різновид інформаційних війн.
57. Види та характерні риси кібервійн.
58. Захист кіберпростору України.

Шкала оцінювання знань здобувачів освіти з формою контролю – залік

Оцінка в балах	Лінгвістична оцінка
90 – 100	Зараховано
82 – 89	
75 – 81	
67 – 74	
60 – 66	
1 – 59	Незараховано (необхідне перескладання)

Вирішення конфліктних ситуацій

Будь-яка конфліктна ситуація, яка виникає в учасників освітнього процесу вирішується згідно Положення про порядок і процедури вирішення конфліктних ситуацій у ВНУ імені Лесі Українки

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, **Статуту** і **Правил внутрішнього розпорядку ВНУ імені Лесі Українки**, загально-прийнятих 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 та списування. Очікується, що всі здобувачі освіти відвідають усі лекції і лабораторні заняття освітнього компоненту.

Політика щодо академічної доброчесності

Політика, стандарти та процедури дотримання академічної доброчесності у Волинському національному університеті імені Лесі Українки знайшли своє відображення в «Кодексі академічної доброчесності Волинського національного університету імені Лесі Українки». Вимоги до академічної доброчесності визначаються «Положенням про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Волинського національного університету імені Лесі Українки».

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.

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. Або прикріпити звіт виконання завдань у відповідне дистанційне середовище.

Рекомендована література та інтернет-ресурси

1. Сілін Є.С. Конспект лекцій із навчальної дисципліни СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ (З ЕЛЕМЕНТАМИ КІБЕРБЕЗПЕКИ). 2023. 182 с.
2. Сілін Є.С. Методичні вказівки до виконання лабораторних робіт із навчальної дисципліни СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ (З ЕЛЕМЕНТАМИ КІБЕРБЕЗПЕКИ). 2023. 154 с.
3. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020. 678 с.
4. Тарнавський Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки»; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
5. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. 177 с.
6. Карачка А. Ф. Технології захисту інформації. Текст лекцій. Тернопіль: ТНЕУ, 2017. 86 с.
7. Онлайн-курс «Основи інформаційної безпеки». Prometheus. *Prometheus*. URL: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about

8. Онлайн-курс «Захист персональних даних». Ed-era. URL: https://www.ed-era.com/courses/
9. Інформатика в прикладах – Основні види шкідливого програмного забезпечення. *Інформатика в прикладах - Головна*. URL: http://nikolay.in.ua/do-uroku/informatsijna-bezpeka/564-osnovni-vidi-shkidlivogo-programnogo-zabezpechennya
10. Снопченко Д. Безпека в соціальних мережах – етика поведінки в інтернеті. *ms.detector.media*. URL: https://ms.detector.media/profstandarti/post/2369/2013-11-18-bezpeka-v-sotsialnykh-merezhakh-etyka-povedinky-v-interneti/
11. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах *ELAKPI: Home*. URL: https://ela.kpi.ua/bitstream/123456789/18028/1/30_p14.pdf
12. CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/recommendation/31

Перелік нормативно-правових актів

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

Погоджено

Гарант освітньо-професійної програми:  Світлана ЯЦЮК

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

протокол № 1 від 30 серпня 2023 р.

Завідувач кафедри:  Тетяна ГРИШАНОВИЧ