МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента

ОСНОВИ КІБЕРБЕЗПЕКИ

підготовки бакалавра

Луцьк – 2026

Силабус освітнього компонента «Основи кібербезпеки**»** підготовки бакалавра, всіх галузей знань, всіх спеціальностей, за всіма освітніми програмами.

Розробник: Глинчук Л. Я., доцент кафедри комп'ютерних наук та кібербезпеки, кандидат фізико-математичних наук, доцент.

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

протокол № 6 від 15.01.2026 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 2
150/5 кредитів	Семестр 4
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: немає	Консультації 10 год.
	Форма контролю: залік

ІІ. Інформація про викладача

ПІП Глинчук Людмила Ярославівна
Науковий ступінь кандидат фізико-математичних наук
Вчене звання доцент
Посада доцент кафедри комп'ютерних наук та кібербезпеки
Контактна інформація номер моб. тел.: 0958904246,
ел. скринька: hlynchuk.ludmila@vnu.edu.ua
Дні занять -

ІІІ. Опис освітнього компонента

1. **Анотація освітнього компонента.**
   Силабус вибіркового освітнього компонента «Основи кібербезпеки» складено з урахуванням можливості формування індивідуальної освітньої траєкторії здобувачів освіти підготовки бакалавра. Знайомить з основними принципами безпечної роботи на ПК та в мережі.

2. **Пререквізити.**
   Знання та вміння, отримані в результаті вивчення дисциплін по напрямах ІТ.
   Постреквізити. Знання та вміння, отримані в результаті вивчення дисципліни, можуть бути корисні при вирішенні задач інформаційного захисту, кіберебезпеки, кібергігієни. Для того аби вміти використовувати відповідне програмне забезпечення та інтернет-ресурси для виконання завдань даного напряму.

3. **Мета і завдання освітнього компонента.**
   Мета дисципліни: сформувати знання, вміння та навички, необхідні для ефективного використання програмних засобів та інтернет-ресурсів у майбутній професійній діяльності та для організації безпечного середовища власного користування.
   Завдання:
   - виробити здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійній діяльності;

- навчитися підбирати програмні технології для захищеної роботи на ПК та в мережі;
- навчитися уникати небезпеку в інформаційному просторі;
- забезпечувати захист і збереження власних персональних даних.

4. Soft skills.

Критичне та системне мислення – аналіз загроз, пошук рішень.
Комунікація і командна робота – виконання завдань в парах, підготовка звітів.
Етична відповідальність – усвідомлення важливості приватності й правил кібергігієни.
Прийняття рішень і розв'язання проблем – вибір оптимальних способів реагування на інциденти.
Адаптивність і самоорганізація – підтримка власної кібербезпеки, навчання новому.

5. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю / Бали
Змістовий модуль 1. Основи та елементи кібербезпеки						
Тема 1. Вступ в кібербезпеку, основні поняття. Види вторгнень. Законодавство України у даній сфері. Кіберзброя та кіберзлочинність.	14	2	2	8	2	Звіт/4
Тема 2. Аутентифікація. Паролі, правила створення та керування.	16	2	4	8	2	Звіт/6
Тема 3. Резервні копії. Видалення/відновлення даних. Захист даних.	16	2	4	8	2	Звіт/8
Тема 4. Види шкідливого програмного забезпечення та захист від нього. Соціальна інженерія. Діагностика ПК.	18	2	6	8	2	Звіт/11
Тема 5. Кібербезпека в мережі. Безпека в соціальних мережах. Основні правила кібергігієни.	16	2	4	8	2	Звіт/6
Разом за модулем 1	80	10	20	40	10	35
Тестування				6		20
Самостійна робота студента				64		45
Всього годин/Балів	150	10	20	110	10	100

6. Завдання для самостійного опрацювання.

№ з/п	Тема (опрацювати)	Кількість годин/бал
1.	Опрацювання та аналіз лекційного матеріалу	10
2.	Підготовка до лабораторних робіт	20

3.	Робота з відповідними інтернет-ресурсами	10
4.	Підготовка до тестування	6
5.	Дослідити законодавчі інновації останніх років у сфері кібербезпеки	4 год./3 б.
6.	Пройти онлайн курс «Аналітик з кібербезпеки» https://osvita.diia.gov.ua/courses/cybersecurity-analyst	5 год./4 б.
7.	Проходження онлайн-курсу «Кіберняні» (результат Сертифікат) https://osvita.diia.gov.ua/courses/cybernanny	6 год./4 б.
8.	Виконати відновлення втрачених даних на власному ПК за допомогою безкоштовних спеціалізованих програм. Обрати для виконання завдання мінімум 2 спеціалізовані безкоштовні програми.	7 год./4 б.
9.	Виконати видалення без можливості відновлення на власному ПК: - використовуючи можливості вашої ОС; - використовуючи спеціальну безкоштовну програму.	5 год./3 б.
10.	Виконати шифрування файлів на власному ПК будь якою безкоштовною програмою.	4 год./3 б.
11.	Виконати перевірку ПК за допомогою одного з онлайн-сканерів (завантажити) та продемонструвати три типи антивірусних перевірок (швидке, повне, вибіркове сканування) та показати, що дане ПЗ може працювати поряд з основним антивірусом вашого ПК: https://www.eset.com/ua-ru/home/online-scanner https://zillya.ua/zillya-skaner	7 год./4 б.
12.	Користуючись джерелами https://uk.soringpcrepair.com/computer-diagnostic-software/, https://programy.com.ua/ua/diagnostic/, розглянути програми для діагностики ПК. Для виконання завдання діагностики власного ПК використайте безкоштовну, наприклад, CPU-Z (http://hi-news.pp.ua/kompyuteri/14061-cpu-z-yak-koristuvatisya-opis-programi-ta-mozhlivost.html), або будь яку іншу, оберіть самі згідно ваших інтересів та необхідності. Для завдання використати 2 ПЗ.	6 год./4 б.
13.	Пройти онлайн курс «Кібергігієна: як захиститися від фішингу» (результат Сертифікат) https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu	4 год./4 б.
14.	Проходження онлайн-курсу «Основи кібергігієни» (результат Сертифікат) https://osvita.diia.gov.ua/courses/cyber-hygiene	10 год./7 б.
15.	Проходження онлайн-курсу «Кібергігієна для молоді» (результат Сертифікат) https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth	6 год./5 б.
Разом		110 год.

IV. Політика оцінювання

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; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання 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.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми.

Під час модульного та підсумкового контролю (заліку) студентам заборонено користуються такими засобами як мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання мають бути виконані у встановлений термін. Несвоєчасно виконані завдання оцінюються на нижчу оцінку. Виключенням можуть бути завдання, які не вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, то він (вона) вивчає матеріал самостійно, використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу, у випадку розміщення його на платформі дистанційного навчання Moodle, виконує всі домашні завдання (завдання подані на самостійну роботу). Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс, прикріпивши виконанні завдання у відповідні комірки та попередити викладача про здане завдання, або під час консультацій або надіслати виконане завдання на корпоративну пошту викладача. Зворотній зв'язок з викладачем для з’ясування всіх питань: використання форуму, чату дистанційного курсу, корпоративної пошти університету або відповідної бесіди у певному месенджері.

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті

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».

Можливість отримати додаткові (бонусні) бали

Відповідно до пункту 4.5 Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки здобувачам освіти, які брали участь у роботі конференцій, підготовці наукових публікацій, в олімпіадах, конкурсах студентських наукових робіт, спортивних змаганнях, мистецьких конкурсах тощо й досягли значних результатів, може бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю з відповідного ОК. Систему бонусних балів погоджує науково-методична комісія факультету (інституту).

І так, здобувачі освіти мають можливість отримати додаткові бали за вказаний вид робіт з ОК «Основи кібербезпеки» відповідно до таблиці витягу з протоколу № 1 засідання НМТ ФІТІМ ВНУ ім. Лесі Українки від 3.09.2025 р.

Системи бонусних балів для здобувачів освіти

Вид діяльності	Рівень / результат	Кількість бонусних балів
Студентські олімпіади	І місце	7
	ІІ місце	5
	ІІІ місце	3
	Участь в олімпіаді	2
Конкурси студентських наукових робіт	Диплом І ступеня	7
	Диплом ІІ ступеня	5
	Диплом ІІІ ступеня	3
Підготовка наукових публікацій	Публікація в WoS / Scopus	10
	Фахова стаття	7
	Нефахова стаття	5
	Публікація тез	2
Участь у конференціях	Виступ на конференції	2
Першість України з командного програмування	І місце	10
	ІІ місце	8
	ІІІ місце	6
	Участь	4

V. Підсумковий контроль

Підсумковий контроль з даної дисципліни передбачено у вигляді заліку.

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, тестових робіт та виконання самостійної роботи. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання, у випадку заліку, за семестр – 100 балів.

Залік викладач виставляє за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом ОК. У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, 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 залік під час ліквідації академічної заборгованості, як правило, 100. У день складання заліку за основною сесією заборонено проводити додаткові опитування здобувача освіти, а також здобувач освіти не має права доздавати будь-який вид робіт, передбачений силабусом освітнього компоненту. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонента. Порядок проведення заліку-ліквідації – залік відбувається у вигляді виконання комплексного завдання.

Питання до заліку та приклади практичних завдань
(у випадку ліквідації академічної заборгованості)

1. Основні поняття: захист інформації, інформаційна безпека, кібербезпека, кібергігієна. Види вторгнень.
2. Нормативно-правове регулювання інформаційної безпеки в Україні.
3. Закон України «Про основні засади забезпечення кібербезпеки України»
4. Закон України «Про захист персональних даних».
5. Кіберзброя та кіберзлочинність.
6. Аутентифікація/двохфакторна аутентифікація користувача.
7. Технології захисту мобільних телефонів на рівні пристрою.
8. Правила для створення надійного та стійкого паролю. Методи злому паролю. Методи створення стійких паролів.
9. Сервіси для перевірки стійкості паролів, менеджери паролів
10. Резервне копіювання та його класифікація. Рівні зберігання резервних копій.
11. Особливості видалення/відновлення даних.
12. Основи криптографії та стеганографії.
13. Основні види шкідливих програм. Джерела зараження шкідливим ПЗ та ознаки зараження ПК.
14. Технології захисту: сигнатурний, статичний, динамічний аналіз.
15. Гібридний підхід, евристичний та поведінковий аналізатор. Репутаційні технології. Хмарні технології.
16. Що робити при зараженні пристрою шкідливим ПЗ? Сторона законодавства у сфері шкідливого ПЗ.
17. Методи соціальної інженерії.
18. Спам. Фішинг.
19. Особливості діагностики ПК. Програмні засоби для діагностування ПК.
20. Безпека в браузерах. Корисні плагіни для додаткового блокування та захисту.
21. Технології Proxy. Особливості віртуальної приватної мережі (VPN).
22. Фільтр доменних імен (DNSFilter), міжмережевий екран (Firewall). Правила роботи у Wi-Fi.
23. Цифровий слід (digital footprint).
24. Безпека в соціальних мережах – етика поведінки в інтернеті (поради експертів).
25. Основні правила кібергігієни від CERT-UA.

Приклади практичних завдань

1. Налаштувати двохфакторну автентифікацію акаунту або в Google або на власному мобільному пристрої. Результат продемонструвати. Після виконання завдання двохфакторну авторизацію можна видалити.
2. Налаштувати резервне копіювання та відновлення в ОС. Налаштувати резервне копіювання на Google диску. Створити резервну копію даних за допомогою хмарного сховища. Результат продемонструвати.
3. Продемонструвати за допомогою тесту https://zillya.ua/check-password перевірку паролю на надійність: підберіть паролі різної складності та протестуйте, використайте інші сервіси (хоча б 2), які виконують таке ж саме тестування на надійність (результат перевірки продемонструвати).
4. Для створення складних паролів можна використовувати сервіси генерації паролів, як-от на сайті кіберполіції: https://www.cyberpolice.gov.ua/generatepassword/ , використайте ще декілька таких сервісів та продемонструйте їх роботу. Продемонструйте роботу в менеджері паролів.

Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є залік

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

VI. Рекомендована література та інтернет-ресурси

1. Кібервійна як різновид інформаційних війн. Захист кіберпростору України / Дмитрук Я.В., Гришанович Т.О., Глинчук Л.Я., Жигаревич О.К. *Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка"*, 2022. 4(16), С. 28-36. URL: https://doi.org/10.28925/2663-4023.2022.16.2836
2. Глинчук Л.Я. Аспекти проєктування систем захисту з орієнтацією на людину. *Наука, освіта, технології і суспільство: світові тенденції та регіональний аспект*: збірник тез доповідей міжн. наук.-практ. конф. (Рівне, 11 січня 2023 р.): у 3 ч. Рівне: ЦФЕНД, 2023. Ч. 3. С. 11-12.
3. Глинчук Л.Я. Технології захисту мобільних телефонів від загроз на рівні пристрою. *Розвиток сучасної науки та освіти: реалії, проблеми якості, інновації*: матеріали IV міжн. наук.-практ. інтернет-конф. (Запоріжжя, 29-31 травня 2023 р.). Запоріжжя: ТДАТУ, 2023. С. 57-62.
4. Глинчук Л.Я. Аналіз та приклади інформаційних атак у месенджері Telegram. *Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем:* тези доповідей І міжн. наук.-практ. конф. (Луцьк-Світязь, 13-16 червня 2024 р.). URL: https://apcssm.vnu.edu.ua/index.php/conf/article/view/30
5. Глинчук Л., Лапчук С. Особливості інтеграції систем захисту даних у програмне забезпечення: від концепції до впровадження. *Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем:* тези доповідей ІІ міжн. наук.-практ. конф. (Луцьк-Світязь, 9-11 червня 2025 р.). URL: https://apcssm.vnu.edu.ua/index.php/conf/article/view/163/158
6. Сілін Є.С. Конспект лекцій із навчальної дисципліни СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ (З ЕЛЕМЕНТАМИ КІБЕРБЕЗПЕКИ). 2023. 182 с.
7. Сілін Є.С. Методичні вказівки до виконання лабораторних робіт із навчальної дисципліни СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ (З ЕЛЕМЕНТАМИ КІБЕРБЕЗПЕКИ). 2023. 154 с.
8. Онлайн-курс «Основи інформаційної безпеки». Prometheus. *Prometheus*. URL: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about
9. Основи кібергігієни. *Дія. Цифрова Освіта*. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene

10. Онлайн-курс «Інформаційна гігієна під час війни». Prometheus. *Prometheus*. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IHWAR101+2022_T2/about
11. 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
12. 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/
13. 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
14. CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/recommendation/31

Інтернет-ресурси для лабораторних робіт

Онлайн-курс «Захист персональних даних»
https://www.ed-era.com/courses/
Приховування (стеганографія) даних (онлайн-інструмент +декодер)
https://tools.icoder.uz/image-steganography.php
https://stylesuxx.github.io/steganography/
https://manytools.org/hacker-tools/steganography-encode-text-into-image/
генератори паролів:
https://www.avast.ua/random-password-generator,
https://1password.com/password-generator/,
https://axcrypt.net/information/password-generator,
https://www.cyberpolice.gov.ua/generatepassword/;
створення карти паролів: https://www.savernova.com/;
перевірка надійності паролів:
https://exploit.in/passcheck/,
https://www.security.org/how-secure-is-my-password/,
https://zillya.ua/check-password;
бази паролів, які були скомпрометовані:
https://breachalarm.com/?,
https://pwnedlist.com/query,
https://haveibeenpwned.com/Passwords;
посібник для самостійного вивчення LibreOffice:
http://lpk.ucoz.ua/Informatika/LibreOfficee_posibnik_ua.pdf;
документація та підтримка LibreOfficee:
https://documentation.libreoffice.org/en/english-documentation/,
https://help.libreoffice.org/6.3/uk/text/shared/05/new_help.html;
сервіси відновлення втрачених паролів:
https://www.lostmypass.com,
https://www.password-find.com/;
тести антивірусного програмного забезпечення:
https://www.av-test.org/en/antivirus/home-users/,
https://www.av-comparatives.org/;
хмарні антивірусні сервіси:
https://www.virustotal.com/gui/home/upload,
https://www.hybrid-analysis.com/,

https://metadefender.opswat.com;
онлайн сканери:
https://www.eset.com/ua-ru/home/online-scanner,
https://zillya.ua/zillya-skaner,
https://www.trendmicro.com/ru_ru/forHome/products/housecall.html.
довідкові системи браузерів Google Chrome, Mozilla Firefox, Opera:
https://support.google.com/chrome/?p=help&ctx=settings#topic=9796470,
https://support.mozilla.org/uk/products/firefox?as=u&utm_source=inproduct,
https://help.opera.com/ru/latest/;
додатки для браузерів Google Chrome, Mozilla Firefox, Opera:
https://chrome.google.com/webstore/category/extensions?hl=uk,
https://addons.mozilla.org/uk/firefox/,
https://addons.opera.com/uk/extensions/;
довідка веб-магазину Chrome:
https://support.google.com/chrome_webstore/answer/2664769?hl=uk;
додаткові фільтри для блокувальника uBlock Origin:
https://github.com/search?q=uBlock-filters;
довідник поштових скриньок, які потрапили до баз даних у мережі:
https://haveibeenpwned.com;
тест браузера на рівень інформаційної ентропії:
https://coveryourtracks.eff.org;
як браузер фіксує інформацію щодо переміщення курсора миші:
https://clickclickclick.click/#ab8459dff2c433c3f59108d42618bc9b;
демонстрація даних, які збирає браузер про комп’ютер користувача:
https://webkay.robinlinus.com/
проксі-сервери:
https://www.hidemyass.com/uk-ua/proxy,
https://www.kproxy.com/,
https://www.4everproxy.com/,
http://dontfilter.us/.