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

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

підготовки здобувачів першого (бакалаврського) рівня вищої освіти
галузі знань: 01 Освіта/Педагогіка
спеціальності: 014 Середня освіта (Інформатика)
освітньо-професійної програми: Середня освіта. Інформатика

Луцьк – 2022

Силабус освітнього компонента «Технології захисту інформації**»** підготовки бакалавра, галузі знань 01 Освіта/Педагогіка, спеціальності 014 Середня освіта (Інформатика), за освітньо-професійною програмою Середня освіта. Інформатика

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

Погоджено

Гарант освітньо-професійної програми:  Світлана ЯЦЮК

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

протокол № 2 від 29.09.2022 р.

Завідувач кафедри:  Тетяна ГРИШАНОВИЧ

© Глинчук Л.Я., 2022 р.

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="8">01 Освіта/Педагогіка

014 Середня освіта (Інформатика)

Середня освіта. Інформатика

Перший (бакалаврський)</td><td>Нормативний</td></tr>
<tr><td rowspan="3">Кількість годин/кредитів

120/4</td><td>Рік навчання: IV</td></tr>
<tr><td>Семестр: 8</td></tr>
<tr><td>Лекції: 20 год.</td></tr>
<tr><td rowspan="4">ІНДЗ: немає</td><td>Лабораторні роботи: 30 год.</td></tr>
<tr><td>Самостійна робота: 62 год.</td></tr>
<tr><td>Консультації: 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання</td><td>Українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП **Глинчук Людмила Ярославівна**
Науковий ступінь **кандидат фізико-математичних наук**
Вчене звання -
Посада **доцент кафедри комп'ютерних наук та кібербезпеки**
Контактна інформація **тел.:095 890 42 46, e-mail: Hlynchuk.Ludmila@vnu.edu.ua**
Дні занять **http://194.44.187.20/cgi-bin/timetable.cgi?n=700**

ІІІ. Опис освітнього компонента

1. Анотація курсу. Силабус освітнього компонента «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ» складений відповідно до навчального плану підготовки *БАКАЛАВРА*, галузі знань *01 Освіта/Педагогіка*, спеціальності *014 Середня освіта (Інформатика)*, освітньо-професійної програми С*ередня освіта. Інформатика.* Його вивчення 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.

2. Предреквізити. Базові знання з ОК: «Програмування», «Прикладне програмне забезпечення а хмарні технології», «Теорія ймовірностей та математична статистика», «Системне програмування та операційні системи», «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.

3. Мета і завдання. 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 крипрографічного захисту.

Процес вивчення ОК спрямований на формування елементів наступних загальних (ЗК) та спеціальних (СК) ***компетентностей***:

ЗК 7. Здатність знаходити, обробляти, інформацію з різних джерел, аналізувати та синтезувати на основі перевірених фактів та логічних аргументів.

ЗК 8. Здатність до самовизначення мети діяльності, самостійного пошуку знань, їх осмислення, закріплення, формування та розвитку умінь і навичок.

ЗК 10. Здатність застосовувати навички використання інформаційних і комунікаційних технологій.

ЗК 11. Здатність до генерування нових ідей, виявлення та розв’язання проблем, ініціативності та підприємливості.

СК 1. Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійній діяльності.

СК 5. Здатність застосовувати сучасні інформаційно-комунікаційні та Internet-технології для управління та забезпечення якості навчально-виховного процесу в середніх закладах освіти.

СК 23. Здатність проводити адміністрування комп’ютерної мережі, реалізовувати комплекс заходів, спрямованих на забезпечення захисту інформації та формування вмінь безпечної роботи школярів у комп’ютерній мережі.

СК 25. Здатність раціонально використовувати комп’ютери, мережеві технології та програмні середовища для розв’язування навчальних, професійних і життєвих завдань.

Опанування змісту освітнього компонента дозволяє отримати наступні результати навчання:

ПР 23. Розуміти концепцію інформаційної безпеки, забезпечувати безпеку інформаційних мереж в умовах неповноти та невизначеності вихідних даних.

ПР 25. Підбирати програмно-апаратні засоби, програмні технології та сучасні інформаційні системи для улаштування комп’ютерного класу, дотримуючись вимог до освітлення, мікроклімату, електро та пожежної безпеки на основі знань принципів побудови інформаційних систем та організації захисту інформації.

4. Структура освітнього компонента

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	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	10	2	2	6		ІРС/3
Тема 2. Стандарти у галузі оцінки захищеності комп'ютерних систем. Поняття та захист авторського права. Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіату	11	2	2	6	1	ІРС/3
Тема 3. Захист інформації засобами операційної системи. Використання паролів і механізмів контролю за доступом. Поняття батьківського контролю	13	2	4	6	1	ІРС/6
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	ІРС/3
Тема 5. Огляд методів виявлення шкідливих програм. Класифікація та можливості антивірусного ПЗ. Огляд найпоширенішого ПЗ даного типу	13	2	4	6	1	ІРС/5
Разом за модулем 1	**58**	**10**	**14**	**30**	**4**	**ІРС/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. Міжмережеві екрани, їх функції та види. VPN-сервіс. Інформаційна безпека в соціальних мережах.	13	2	4	6	1	ІРС/5

Тема 7. Технічний та інженерний захист інформації. Канали витоку інформації. Нормативні документи технічного захисту інформації	11	2	2	6	1	ІРС/3
Тема 8. Криптографічний вид захисту інформації: симетричні та асиметричні алгоритми. Цифровий підпис. Програмне забезпечення для здійснення шифрування інформації	9	2	4	2	1	ІРС/6
Тема 9. Системи виявлення та запобігання вторгнень. SIEM-системи. Тестування на проникнення	15	2	4	8	1	ІРС/4
Тема 10. Особливості біометричного захисту інформації. Біометричні технології	10	2	2	6		ІРС/2
Разом за модулем 2	**62**	**10**	**16**	**32**	**4**	**ІРС/20**
Види підсумкових робіт						Бал
Контрольна робота № 1						15
Контрольна робота № 2						15
Індивідуальна робота студента*						30
Всього годин/ Балів	**120**	**20**	**30**	**62**	**8**	**100**

Індивідуальна робота студента* виставляється за наявності сертифікатів з онлайн-курсів поданих на самостійне опрацювання (8, 7, 7, 4, 4 балів відповідно за курс)

5. 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 «Захист персональних даних» платформа https://www.ed-era.com/courses/
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.	Опрацювання лекційного матеріалу
7.	Виконання лабораторних робіт

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Оцінювання здійснюється згідно «ПОЛОЖЕННЯ про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки». 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 здобувачі освіти відвідають усі лекції і лабораторні 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 написання контрольної роботи та складання заліку здобувачам освіти 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. 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.

V. Підсумковий контроль

Підсумковий контроль з освітнього компонента передбачено у вигляді **заліку**.

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль, який нараховується за виконання лабораторних робіт, індивідуальних робіт, контрольних робіт, тестових робіт до лекційних матеріалів курсу (форми контролю та бали за них прописані в останньому стовпці таблиці «Структура освітнього компонента»). Максимальна кількість балів, яку може отримати здобувач освіти під час поточного оцінювання за семестр – 100 балів. 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.

Порядок проведення заліку-ліквідації – залік відбувається у вигляді виконання практичного завдання та відповіді на теоретичні питання.

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. Поняття батьківського контролю та його налаштування.
16. Поняття шкідливого програмного забезпечення, його види. Як працює та як проявляється.
17. Соціальна інженерія, її види та особливості.
18. Небезпека для дітей в мережі Інтернет.
19. Що таке комп'ютерний вірус? Де подивитися бібліотеку вірусів?
20. Що таке троянське зловмисне програмне забезпечення?
21. Що таке шпигунське програмне забезпечення?
22. Що таке вимагацьке програмне забезпечення?
23. Відповідальність за створення, розповсюдження та використання шкідливого ПЗ.
24. Класифікація антивірусного ПЗ. Його особливості та функції.
25. Огляд найпоширенішого антивірусного ПЗ. Приклади.
26. Хмарний чи традиційний антивірус? Плюси та мінуси.
27. Основи безпеки інформації в комп'ютерних мережах.
28. Міжмережеві екрани, їх функції та види.
29. VPN-сервіс, особливості та приклади.
30. Інформаційна безпека в соціальних мережах.
31. Протоколи безпеки Інтернет, протокол Kerberos.
32. Технічний та інженерний захист інформації. Ринок приладів для захисту.
33. Канали витоку інформації.
34. Нормативні документи технічного захисту інформації.
35. Криптографічний вид захисту інформації. Основні методи та можливості.
36. Поняття шифрування файлів, папок, повідомлень.
37. Програмне забезпечення для здійснення шифрування інформації.

38. Системи виявлення та запобігання вторгнень.
39. SIEM-системи, їх функції та особливості.
40. Тестування на проникнення.
41. Основні поняття про біометрію. Біометричні характеристики людини.
42. Біометричні системи та технології.
43. Приклади біометричних систем (Ринок цін, зовн. вигляд, функції).
44. Огляд ПЗ для обробки біометричних даних.

Приклади практичних завдань

1. Розказати про плагіат та його види. Продемонструвати роботу з програмним забезпеченням, яке виявляє плагіат. Пояснити результати.
2. Продемонструвати всі можливості вашої ОС для захисту.
3. Створити новий обліковий запис (нового користувача) у вашій ОС, надати йому дозволи та закрити певні доступи. Продемонструвати роботу цього користувача в системі, тобто як відображаються дозволи та заборони.
4. Продемонструвати налаштування батьківського контролю або за допомогою ОС, або за допомогою іншого безкоштовного програмного забезпечення (обрати відповідне).
5. Розказати про відповідальність за створення, розповсюдження та використання шкідливого ПЗ, основні та важливі моменти згідно законодавства. Що зробити якщо вас звинувачують безпідставно?
6. Продемонструвати налаштування та функції (зміну налаштувань) антивірусного програмного забезпечення, яке встановлене на вашому ПК.
7. Продемонструвати роботу антивірусного програмного забезпечення для пошуку шкідливого програмного забезпечення. Прокоментувати результати роботи.
8. Продемонструвати налаштування брандмауера або у вашій ОС або іншого брандмауера встановленого на вашому ПК.
9. Протестувати роботу брандмауера за допомогою спеціального тестуючого програмного забезпечення.
10. Продемонструвати роботу з програмним забезпеченням, яке шифрує диски, папки та файли.

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)

VI. Рекомендована література та інтернет-ресурси

1. Онлайн-курс «Основи інформаційної безпеки». URL: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about
2. Серіал для батьків «Безпека дітей в інтернеті»/ Онлайн-курс. URL: https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey

3. Серіал для батьків «Кіберняні»/ Онлайн-курс. URL: https://osvita.diia.gov.ua/courses/cybernanny
4. Серіал для батьків «Основи кібергігієни»/ Онлайн-курс. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene
5. Онлайн-курс ««Інформаційна гігієна під час війни». URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IHWAR101+2022_T2/about
6. Онлайн-курс «Захист персональних даних». URL: https://study.ed-era.com/uk/courses/course/371
7. 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.
8. 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.