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

СИЛАБУС
нормативної навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЇ

підготовки бакалавра

галузей знань 12 «Інформаційні технології»,
01 «Середня освіта»,
11 «Математика та статистика»

спеціальностей 122 «Комп'ютерні науки»,
014 «Середня освіта (Інформатика)»
113 «Прикладна математика»

освітньо-професійних програм
«Комп'ютерні науки та інформаційні технології»,
«Середня освіта. Інформатика»,
«Прикладна математика»

Луцьк – 2021

Силабус навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ» підготовки бакалавра, галузей знань 12 «Інформаційні технології», 01 «Середня освіта», 11 «Математика та статистика» спеціальностей 122 «Комп'ютерні науки», 014 «Середня освіта (Інформатика)», 113 «Прикладна математика» за освітньо-професійними програмами «Комп'ютерні науки та інформаційні технології», «Середня освіта. Інформатика», «Прикладна математика».

Розробник: Глинчук Людмила Ярославівна, кандидат фізико-математичних наук, кафедри комп'ютерних наук та кібербезпеки

Силабус навчальної дисципліни затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 7 від 5 січня 2021 р.

В. о. завідувача кафедри  Гришанович Т.О.

І. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td>Шифр і назва галузі знань:
12 Інформаційні технології
01 Середня освіта
11 Математика та статистика</td><td rowspan="2">Нормативна</td></tr>
<tr><td>Напрям підготовки:
122 Комп’ютерні науки
014 Середня освіта (Інформатика)
113 Прикладна математика</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів
90/3</td><td rowspan="4">Освітньо-професійна програма
Комп’ютерні науки та інформаційні технології
Середня освіта. Інформатика
Прикладна математика</td><td>Рік навчання: IV</td></tr>
<tr><td>Семестр: 8</td></tr>
<tr><td>Лекції: 28 год.</td></tr>
<tr><td>Лабораторні роботи: 28 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td rowspan="3">Освітній ступінь
Бакалавр</td><td>Самостійна робота: 26 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**

Захист інформації. Дистанційний курс в середовищі Moodle: http://194.44.187.60/moodle/course/view.php?id=1386

III. Опис дисципліни

1. **Анотація курсу.** Дисципліна «ЗАХИСТ ІНФОРМАЦІЇ» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра. Спрямована на підвищення рівня формування у студентів знань та умінь, які дадуть теоретичний і практичний фундамент, необхідний для аналізу виникаючих загроз при зберіганні, обробленні та передачі інформації.

2. **Предреквізити.** Базові знання з дисциплін: «Системне програмування та операційні системи», «Інформаційні мережі», «Організація та обробка електронної інформації», «Основи криптології».

3. **Постреквізити.** Знання та вміння, набуті в результаті вивчення дисципліни, можна використати у професійній діяльності з використанням різного виду захисту інформації. А також, для написання випускних кваліфікаційних робіт (бакалаврської, магістерської).

4. **Мета і завдання навчальної дисципліни.**
   Мета викладання навчальної дисципліни "Захист інформації" полягає у комплексному викладі теоретичних основ та практичного використання сучасних видів захисту інформації і технологій згідно із загальними підходами в Україні та світі. Розглядаються поняття, класифікація, сфери застосування, складові і ознаки, різні типи підходів, систем і способі захисту інформаційних ресурсів, а також методи використання інформаційних технологій, їх застосування в різних сферах сучасного життя.
   Завдання: основними завданнями вивчення дисципліни "Захист інформації" є дати наступні **знання**: критерії оцінки інформаційної безпеки; поняття батьківського контролю; найпоширеніші мобільні віруси та засоби боротьби з ними; способи та можливості захисту в соціальних мережах; управління паролями та правила роботи з ними; поняття шкідливого програмного забезпечення; основні типи та загальний огляд сучасних комп'ютерних вірусів; поняття антивірусної програми та їх класифікацію; основи криптографічного захисту; основи біометричного захисту; як забезпечується захист інформації в комп'ютерних мережах; поняття авторського права та плагіату; **та вміння**: користуватися засобами резервного копіювання та відновлення даних; пристроями відновлення даних; користуватися можливостями операційної системи для захисту та налаштовувати власний профіль; захищати інформацію на мобільних телефонах; захистити електронну пошту та власні акаунти під час роботи в мережі; користуватися та налаштовувати антивірусні програми; застосовувати програмне забезпечення з використанням криптографії; захищати інформацію в базах даних; захищати файли різних форматів; захищати авторські права; виявляти плагіат.

Результати навчання (Компетентності) відповідно до освітньо-професійної програми

ЗК Здатність застосовувати знання у практичних ситуаціях.

ЗК Здатність вчитися й оволодівати сучасними знаннями.

ЗК Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

ПРН Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Результати навчання (Компетентності) відповідно до освітньо-професійної програми 2017 р. спеціальності 014:

ЗК 8, 9, 14, 15

Знання та розуміння предметної області та розуміння професії.

Здатність бути критичним і самокритичним при прийнятті обґрунтованих рішень та оцінюванні якості виконуваних робіт.

Навички використання інформаційних і комунікаційних технологій.

Здатність діяти на основі етичних міркувань (мотивів).

СК 12

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.

ПРН 1, 20

Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області.

Організовувати навчально-дослідницьку діяльність, планувати організацію і проведення наукових досліджень у галузі інформатики, математики та інформаційних технологій, оцінювати важливість того чи іншого навчального матеріалу для досягнення основних вимог предметної спеціалізації «Інформатика та математика».

5. Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Захист інформації: законодавство, засоби захисту ОС, шкідливе ПЗ, захист в мережах						

Тема 1. Поняття захисту інформації та інформаційної безпеки. Основні критерії оцінки інформаційної безпеки. Законодавство України у сфері захисту інформації	4	2	2			ІРС/3
Тема 2. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних	5	2	2		1	ІРС/2,5
Тема 3. Захист інформації засобами різних операційних систем. Підходи до побудови захищених ОС. Налаштування власного профілю. Поняття батьківського контролю	4	2	2			ІРС/2,5
Тема 4. Поняття шкідливого програмного забезпечення та антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація	5	2	2		1	ІРС/2,5
Тема 5. Захист інформації на мобільних телефонах. Огляд найпоширеніших мобільних вірусів та засобів боротьби з ними	4	2	2			ІРС/3
Тема 6. Основи безпеки інформації в комп'ютерних мережах та поняття особистої безпеки користувача персонального комп’ютеру. Управління паролями та правила роботи з ними	6	2	2		2	ІРС/3
Тема 7. Інформаційна безпека в соціальних мережах. Захист електронної пошти та власних акаунтів під час роботи в мережі	4	2	2			ІРС/3
Разом за модулем 1	**32**	**14**	**14**		**4**	**ІРС/19,5**
Змістовий модуль 2. Інші практичні види захисту. Авторське право та плагіат						
Тема 8. Технічний та інженерний захист інформації. Нормативні документи технічного захисту інформації. Стандарти захисту інформації	4	2	2			ІРС/3
Тема 9. Криптографічний вид захисту інформації. Поняття шифрування файлів, папок,	4	2	2		1	ІРС/3

повідомлень. Засоби здійснення шифрування інформації						
Тема 10. Захист інформації в базах даних: основні та додаткові методи. Моделі безпеки БД	4	2	2			ІРС/3
Тема 11. Захист файлів різних форматів: doc, pdf, xls та інших	6	2	2		2	ІРС/3
Тема 12. Системи моніторингу загроз, їх функції та особливості	4	2	2		1	ІРС/3
Тема 13. Особливості біометричного захисту інформації. Біометричні технології	4	2	2			ІРС/3
Тема 14. Поняття та захист авторського права. Поняття комп'ютерного піратства. Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіату	4	2	2			ІРС/2,5
Разом за модулем 2	**32**	**14**	**14**		**4**	**ІРС/20,5**
Види підсумкових робіт						Бал
Модульна контрольна робота № 1						30
Модульна контрольна робота № 2 /ІРС						30
Всього годин/ Балів	**64**	**28**	**28**		**8**	**100**

6. Завдання для самостійного опрацювання

№	Тема
1.	Загальні принципи захисту програм від несанкціонованого дослідження
2.	Захист від дизасемблювання
3.	Захист від несанкціонованого налагоджування
4.	Сучасні технології дампінга і захист від нього
5.	Забезпечення безпеки об'єктів інформаційної сфери держави
6.	Режимний характер роботи організації як основа комплексного захисту інформації
7.	Аудит об'єктів ІБ. Аналіз ринків корпоративних ІС
8.	Міжнародний стандарт безпеки ISO/IEC 17799
9.	Захист інформації від витоку технічними каналами. Прилади та комплекси

IV. Політика оцінювання

Оцінювання

Оцінювання навчальних досягнень з дисципліни здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та модульний контроль (оцінюються модульні

контрольні роботи у вигляді тестів або письмово або у вигляді індивідуальних завдань). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 60 балів. Додаткові бали (бонусні, які можуть замінити бали за інший вид робіт) студенти можуть отримати написавши тези (статтю) на конференцію згідно тем предмету, але за умови, що тези прийняли та опублікували, а викладач надав свій позитивний відгук.

Політика викладача щодо студента

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. 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.

Перескладання модульного контролю (письмового чи тестування) заборонено.

V. Підсумковий контроль

Підсумковий контроль з даної дисципліни передбачено у вигляді заліку.

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 60 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому випадку студент складає залік; максимальна кількість балів, яку можна отримати на заліку – 60 балів. Оцінка за семестр, у випадку складання заліку, є сумою балів поточного контролю та балів, отриманих під час заліку.

Порядок проведення заліку – залік відбувається або у вигляді тестування (складається база питань за весь семестр) або у вигляді практичного завдання та усної відповіді на теоретичні питання.

VI. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	Оцінка
90 – 100	Відмінно
82 – 89	Дуже добре
75 – 81	Добре
67 – 74	Задовільно
60 – 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси

1. Дистанційний курс «Основи інформаційної безпеки». [Електронний ресурс]. – Режим доступу: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about
2. Серіал для батьків «Безпека дітей в інтернеті»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey
3. Серіал для батьків «Кіберняні»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/cybernanny
4. Серіал для батьків «Основи кібергігієни»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/cyber-hygiene
5. Глинчук Л.Я. Захист інформації. Дистанційний курс на платформі Moodle ВНУ ім. Лесі Українки. [Електронний ресурс]. – Режим доступу до ресурсу: http://194.44.187.60/moodle/course/view.php?id=1386
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с. [Електронний ресурс]. – Режим доступу до ресурсу: http://dspace.onua.edu.ua/bitstream/handle/11300/11111/%D0%9E%D0%86%D0%91%

20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf?sequence=1&isAllowed=y

7. Ахрамович В.М., Чегренец В.М. Інформаційна безпека. Практикум /В.М. Ахрамович., В.М. Чегренец; Державного університету телекомунікацій. – К.:ДУТ, 2017. – 396 с. іл. – Бібліограф.:393 с.
8. Каплун, В. А. Захист програмного забезпечення. Частина 2: навчальний посібник / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця: ВНТУ, 2014. – 105 с.
9. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань: [б.в.], 2012. – 120 с.
10. Список нормативних документів щодо інформаційної безпеки в Україні. [Електронний ресурс], Вікіпедія.
11. Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 2 – Комплекси технічного захисту інформації Навч. посібник / Д. В. Голев, О.Ю. Русляченко, Ю.В. Бєлова, Д.С. Гончарук. За ред. чл.-кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – 184 с