

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Львівський національний університет імені Івана Франка**  
**Факультет прикладної математики та інформатики**  
**Кафедра кібербезпеки**

**Затверджено**

На засіданні кафедри кібербезпеки  
факультету прикладної математики та  
інформатики  
Львівського національного університету  
імені Івана Франка  
(протокол № 15/23 від 29 серпня 2023 р.)



Завідувач кафедри Венгерський П.С.

**Силабус з навчальної дисципліни**  
**“Інформаційна безпека розподілених систем”,**  
**що викладається в межах ОПІ Кібербезпека**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності 125 – Кібербезпека та захист інформації**

**Львів 2023 р.**

<b>Назва дисципліни</b>	Інформаційна безпека розподілених систем
<b>Адреса викладання дисципліни</b>	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики Кафедра кібербезпеки
<b>Галузь знань, шифр та назва спеціальності</b>	12 – інформаційні технології 125 – кібербезпека та захист інформації
<b>Викладачі дисципліни</b>	Брич Тарас Богданович, доцент кафедри кібербезпеки
<b>Контактна інформація викладачів</b>	taras.brych@lnu.edu.ua
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри).
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/admission/specializations">https://ami.lnu.edu.ua/admission/specializations</a>
<b>Інформація про дисципліну</b>	Дисципліна “Інформаційна безпека розподілених систем” є дисципліною за вибором зі спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 6-му семестрі в обсязі 5-и кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Коротка анотація дисципліни</b>	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про безпеку розподілених інформаційних систем, розуміння основних принципів протидії кіберзагрозам.
<b>Мета та цілі дисципліни</b>	Метою курсу є формування у студентів знань про засоби забезпечення безперебійного функціонування розподілених систем, протидії загрозам кібербезпеки, та, у випадку інцидентів, швидкого відновлення працездатності систем.
<b>Література для вивчення дисципліни</b>	<ol style="list-style-type: none"> <li>1. Joe Reis Fundamentals of Data Engineering. Plan and Build Robust Data Systems. - O'Reilly Media. - 2022. - 456 p.</li> <li>2. M. van Steen, A.S. Tanenbaum Distributed Systems: Principles and Paradigms. – Pearson Education, 2016. – 698 p.</li> <li>3. Глоба Л.С. Розробка інформаційних ресурсів та систем, (Том 1: «Розподілені системи», «Розподілені системи. Поняття розподіленого середовища», «Зв’язок», «Процеси», «Іменування», «Синхронізація») - Київ, Видавництво «Політехніка», рекомендовано МОН України, 2014 р., 376 стор.</li> <li>4. Татарчук М.І. Корпоративні інформаційні системи: Навч. посібник. – К.: КНЕУ, 2007. – 291 с.</li> <li>5. <a href="https://csrc.nist.gov/">https://csrc.nist.gov/</a></li> </ol>
<b>Обсяг курсу</b>	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год.

<p><b>Очікувані результати навчання</b></p>	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p><b>знати:</b></p> <p>принципи побудови розподілених систем, забезпечення кібербезпеки розподілених інформаційно-аналітичних систем, стандарти безпеки функціонування таких систем, основні загрози для розподілених інформаційних систем.</p> <p><b>вміти:</b></p> <p>вирішувати завдання захисту інформації, яка обробляється в розподілених інформаційно-аналітичних системах та їх надійного функціонування; проводити профілювання мережі, та загальну оцінку вразливості CVSS; проводити адміністрування системами безпеки, які використовуються в мережі.</p> <p>Курс забезпечує набуття таких компетентностей: КІ, КЗ 2, КЗ 5, КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 7; та програмних результатів навчання: ПРН 2, 3, 4, 5, 6, 10, 12, 13, 14, 15, 16, 17, 18, 28, 29, 35</p>
<p><b>Ключові слова</b></p>	<p>Кібербезпека, кібератака, загроза, вразливість, локальні мережі, розподілені інформаційно-аналітичні системи. криптографічні протоколи, ідентифікація та аутентифікація, IDS, IPS, EDR.</p>
<p><b>Формат курсу</b></p>	<p>змішаний Проведення лекцій, лабораторних робіт і консультацій.</p>
<p><b>Теми</b></p>	<p>Тема 1. Основні загрози для розподілених інформаційних систем. Міжнародні, корпоративні стандарти забезпечення функціонування інформаційних систем.</p> <p>Тема 2. Основні методи та засоби забезпечення кібербезпеки розподілених інформаційних систем.</p> <p>Тема 3. Криптографічні методи, які використовуються для захисту розподілених інформаційних систем.</p> <p>Тема 4. Автентифікація, ідентифікація та аудит при доступі до розподілених інформаційних систем.</p> <p>Тема 5. Безпека в мережних каналах розподілених інформаційних систем. Криптографічні протоколи.</p> <p>Тема 6. Архітектура локальних мереж, віртуальні мережі, мережні екрани, VPN як складові системи захисту розподілених інформаційних систем</p> <p>Тема 7. Безпека комерційних операцій.</p>
<p><b>Підсумковий контроль, форма</b></p>	<p>залік у кінці семестру</p>
<p><b>Пререквізити</b></p>	<p>Для вивчення курсу студенти потребують базових знань з:</p> <ul style="list-style-type: none"> <li>- Безпека комп'ютерних мереж</li> <li>- Менеджмент інформаційної безпеки</li> <li>- Захист інформації в комп'ютерних мережах</li> </ul>
<p><b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b></p>	<p>Презентації, лекції. Модульний контроль</p>
<p><b>Необхідне обладнання</b></p>	<p>Комп'ютери, комп'ютерні системи та мережі. Віртуальні машини. Інтернет ресурси.</p>

<p><b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b></p>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50</li> <li>• Практичні роботи: 50% семестрової оцінки; максимальна кількість балів 50</li> </ul> <p>Підсумкова максимальна кількість балів 100.</p> <p><b>Академічна доброчесність:</b> Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p><b>Відвідання занять</b> є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.</p> <p><b>Література.</b> Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p><b>Політика виставлення балів.</b> Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.</p>
<p><b>Опитування</b></p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.</p>

**Схема курсу " Адміністрування систем захисту інформації "**

<b>Тиж.</b>	<b>Тема, план, короткі тези</b>	<b>Форма діяльності (заняття)</b>	<b>Література</b>	<b>Завдання, год</b>	<b>Термін виконання</b>
1-2	Тема 1. Основні загрози для розподілених інформаційних систем. Міжнародні, корпоративні стандарти забезпечення функціонування інформаційних систем.	лекція, лаб, самостійна робота	[1 -5]	4 8 12	2 тижні
3-4	Тема 2. Основні методи та засоби забезпечення кібербезпеки розподілених інформаційних систем.	лекція, лаб, самостійна робота	[1 -5]	4 8 12	2 тижні
5-6	Тема 3. Криптографічні методи, які використовуються для захисту розподілених інформаційних систем.	лекція, самостійна робота	[1 -5]	6 8 14	2 тижнів
7-8	Тема 4. Автентифікація, ідентифікація та аудит при доступі до розподілених інформаційних систем.	лекція, самостійна робота	[1 -5]	4 8 10	2 тижні
9-10	Тема 5. Безпека в мережних каналах розподілених інформаційних систем. Криптографічні протоколи.	лекція, самостійна робота	[1 -5]	4 8 10	2 тижні
10-12	Тема 6. Архітектура локальних мереж, віртуальні мережі, мережні екрани, VPN як складові системи захисту розподілених інформаційних систем	лекція, лаб, самостійна робота	[1 -5]	4 8 14	3 тижні
13-16	Тема 7. Безпека комерційних операцій.	лекція, лаб, самостійна робота	[1 -5]	4 8 14	3 тижні