**Міжнародний європейський університет**
Європейська школа бізнесу

# СИЛАБУС

## Назва курсу

Безпека програм та даних

## Інформація про курс

**Назва освітньої програми:**

Освітньо-професійна програма «Інженерія програмного забезпечення», обов'язковий освітній компонент

**Опис курсу:**

Останніми роками безпека програмного забезпечення стала предметом великого занепокоєння. У результаті інтеграція безпеки в розробку програмного забезпечення ускладнилася. Розуміння принципів та методів безпеки програмного забезпечення допомагає розробникам виявляти та вимірювати безпеку на різних стадіях життєвого циклу розробки програмного забезпечення, і, як результат, веде до безпечного програмного забезпечення. Щоб створити відповідне програмне забезпечення, потрібно вжити завчасних заходів для оцінки безпеки

**Передумови вивчення (попередні вимоги):**

Програма упорядкована відповідно до анотації освітньо-професійної програми підготовки бакалаврів, базується на вивченні дисциплін «Фізика (вибрані розділи)», «Методи та засоби інформаційних технологій», «Архітектура та проектування програмного забезпечення», «Архітектура комп'ютера», передує вивченню нормативних дисциплін «Конструювання програмного забезпечення», «Емпіричні методи програмної інженерії» . Знання, отримані здобувачами вищої освіти під час вивчення дисципліни «Безпека програм та даних» можуть бути застосовані під час проходження виробничої практики, підготовки кваліфікаційних робіт за спеціальністю.

**Обсяг кредитів/годин:**

5 кредити ЄКТС/ 150 год.

**Ознаки дисципліни**

| Термін викладання | Семестр | Міжнародна дисциплінарна інтеграція | Курс рік (навчання) | Цикли: загальної підготовки/ професійної підготовки/ вільного вибору |
|---|---|---|---|---|
| 1 семестр | 7 семестр | ні | 4 курс | Цикл професійної підготовки |

**Формат навчання:**

Змішане навчання

**Розташування класної кімнати:**

Ауд. 405 https://dist.ieu.edu.ua/course/index.php?categoryid=649

# Інформація про викладача

**Прізвище та ім'я викладача:**

**Шевчук Лариса Дмитрівна,** доктор. пед. наук, професор

**Кафедра**

Кафедра інформаційних технологій

**Місцезнаходження офісу:**

м. Київ, пр-т Академіка Глушкова, 42 В, каб. 509

**Графік роботи та консультування:**

Щовівторка з 12:00 до 16:00

**Електронна пошта викладача:**

larisa_shevchuk@ieu.edu.ua

# Цілі курсу / Результати навчання

**Цілі курсу**

Оволодіння студентами розуміння шляхів змін в структурі суспільного устрою, що відбуваються під впливом цифрових технологій та можливостей розвитку поняття «цифрового громадянства», ставлячи основу для розвитку саморегуляції особистості в епоху Інтернету. Причому йдеться не про звуження, а про розширення можливостей людини, яка може і готова здійснити вибір усвідомлено та відповідально (цифрова свобода особистості).

**Роль навчальної дисципліни у досягненні програмних результатів**

ПР04. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.
ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.
ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

**Результати навчання**

Знати:

- основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки даних;
- основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;
- моделі порушника, основні види атак, принципи лінійного та диференціального криптоаналізу;
- механізми та протоколи керування ключами в інформаційній системі.

Вміти:

- застосувати сучасні блочні симетричні шифри і режими шифрування;
- аналізувати крипостійкість простих симетричних шифрів;
- досліджувати сучасні асиметричні криптосистеми шифрування;
- аналізувати безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP;
- проводити статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за методикою NIST.

# Зміст курсу

Змістовий модуль 1. БЕЗПЕКА І ЗАХИСТ ПРОГРАМ І ДАНИХ

*Тема 1.* Основні поняття безпеки програм та даних. Основні принципи захисту програмного забезпечення.

*Тема 2.* Ідентифікація та автентифікація користувачів. Системи аналізу захищеності мережі.

Змістовий модуль 2. ОСНОВИ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ПРОГРАМ І ДАНИХ

*Тема 3.* Методи та засоби обмеження доступу до програм та даних. Захист програм від несанкціонованого дослідження.

*Тема 4.* Криптографічний захист інформації. Віртуальні приватні мережі.

Змістовий модуль 3. КРИПТОГРАФІЧНИЙ ЗАХСИТ ПРОГРАМ І ДАНИХ

*Тема 5.* Механізми шифрування. Симетричні та несиметричні криптосистеми.

*Тема 6.* Основи технології відкритих ключів (PKI).

*Тема 7.* Основи цифрової стенографії.

*Тема 8.* Основи криптоаналізу.

Змістовий модуль 4. БЕЗПЕКА В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

*Тема 9.* Основні принципи захисту програмного забезпечення. Захист програмного забезпечення в Інтернет-технологіях.

*Тема 10.* Захист персональних даних.

*Тема 11.* Комплексні системи захисту іноформації.

# Матеріали курсу та вимоги

**Книги та матеріали**


1. С. Е. Остапов, С. П. Євсеєв. О. Г. Король. Технології захисту інформації. Чернівці. Видавничий дом “Родовід”, 2014. 428 с.
2. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

3. Літнарович Р.М. Сучасні технології інформаційної безпеки. Навчальний посібник. МЕГУ, Рівне, 2011. 97 с.
4. О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. Захист інформації в інформаційних системах. Методи традиційної криптографії. Харків: Вид. ХНЕУ, 2010. 316 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
6. Дудатьєв А.В., Каплун В.А., Семеренко В.П. Д 81 Захист програмного забезпечення. Частина 1. Навчальний посібник. Вінниця: ВНТУ, 2005. – 140 с.
7. Мельник І. В. Інформаційні комп'ютерні мережі: Навч. посібник для дист. навчання. К.: Вид. Універ. «Україна», 2006. 250 с.

**Технічні вимоги для роботи на курсі**

Щоб отримати доступ до матеріалів курсу, потрібен буде регулярний доступ до комп'ютера та Інтернету. Для успішного вивчення та складання іспиту з навчального курсу, необхідно постійно поетапно ознайомлюватись з матеріалами, розміщеними на дистанційній платформі університету (Moodle) в курсі «Безпека програм та даних». Також потрібно створювати звітні документи на виконання практичних робіт та завантажувати їх на платформу (використання платформи можливе тільки з акаунта корпоративної пошти).
З питань проблем доступу до платформи дистанційного навчання, необхідно повідомити деканат або старосту, або ж безпосередньо викладача курсу.

# Процес навчання

Процес вивчення курсу «Безпека програм та даних» містить лекції та практичні заняття.
Під час лекцій будуть використовуватись такі методи навчання, як лекція, лекція-бесіда, дискусія, обговорення проблемних питань, демонстрація, аналіз різних ситуацій відповідно до теми лекцій.
Під час практичних занять будуть використовуватись такі методи навчання, як опитування, тестування, виконання індивідуальних завдань, виконання аналітично-розрахункових робіт, вирішених конкретних задач та ситуацій.

# Політики оцінювання

**Сумативне оцінювання**

У вас будуть різні способи продемонструвати свої знання і навички протягом семестру. Це включає те, як ви відвідуєте заняття, як і що ви вносите в обговорення тем, як виконуєте і чи вчасно виконуєте лабораторні завдання та тести, як виконуєте завдання з самостійної роботи, вміння презентувати свою роботу. Додатково надається

можливість виконання завдань, які виконуються індивідуально або невеликою групою у вигляді студентської наукової роботи.

| Діяльність протягом семестру | Максимальна кількість балів протягом семестру |
|---|---|
| ПОТОЧНИЙ КОНТРОЛЬ – 60 балів | |
| Поточна робота (відвідування, контроль на лекції) | 8 |
| Виконання практичних робіт (16 шт.) | 32 |
| Виконання самостійних робіт | 10 |
| Виконання індивідуальної роботи | 10 |
| ЕКЗАМЕНАЦІЙНИЙ КОНТРОЛЬ – 40 балів | |
| ВСЬОГО – 100 балів | |

**Шкала оцінювання**

Оцінка за дисципліну визначається як сума набраних балів за поточну діяльність у семестрі та балу за підсумковий контроль. Підсумковий контроль у формі екзамену проводиться після завершення вивчення усіх тем дисципліни і складається здобувачами освіти у період залікової сесії.
Мінімальна кількість балів, яку повинен набрати здобувач освіти за поточну навчальну діяльність за семестр для допуску до підсумкового контролю – 36 балів.
Мінімальна кількість балів за поточну навчальну діяльність та балів за іспит, яка дозволяє зарахувати дисципліну як виконану, має бути не менше 60. Максимальний бал з дисципліни становить 100.
Сумарна оцінка за вивчення дисципліни виставляється за національною та європейською шкалою (ЄКТС).
Загальна підсумкова оцінка в балах, за національною шкалою та за шкалою ЄКТС заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента.

Шкала оцінювання: національна та ЄКТС

| Сума балів за всі види навчальної діяльності | Оцінка ЄКТС | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсового проекту (роботи), практики | для заліку |
| 90-100 | A | відмінно | Зараховано |
| 82-89 | B | добре | |
| 74-81 | C | | |
| 66-73 | D | Задовільно | |
| 60-65 | E | | |
| 30-59 | FX | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного складання |
| 1-29 | F | незадовільно з обов'язковим повторним | не зараховано з обов'язковим повторним вивченням дисципліни |

| | | | | | |
|---|---|---|---|---|---|
| | | | вивченням дисципліни | | |

**Як дізнатись свою оцінку:**

Щоб перевірити свої оцінки за завдання та прочитати коментарі викладача, необхідно перевірити відповідні вкладки на дистанційний платформі навчання (Moodle) у даному курсі.
Також отримати інформацію про отримані оцінки можна в спільному чаті групи з дисципліни (Viber чи Telegram) або безпосередньо у викладача курсу через корпоративну пошту, меседжери або ж за попереднім записом у дні надання консультацій.

# Політики курсу

**Загальні настанови**

Для продуктивної навчально-пізнавальної діяльності здобувачів при вивченні дисципліни здійснюються тематичні лекції та проводяться практичні заняття.
На заняттях та під час перебування в університеті студент повинен поважно ставитися до викладачів, співробітників та інших студентів, відвідувати заняття згідно з розкладом, приходити вчасно і не залишати аудиторії без дозволу викладача. Необхідно виконувати всі академічні завдання і роботи їх у визначені терміни.
Викладач, у свою чергу повинен постійно підвищувати свій професійний рівень, педагогічну майстерність, загальну культуру, забезпечувати умови для засвоєння студентами навчальних програм на рівні обов'язкових вимог щодо змісту, рівня та обсягу освіти, сприяти всебічному професійному розвитку студентів. Обов'язково дотримуватися навчально-тематичного плану, не спізнюватися на заняття, не допускати жодних проявів корупції, дискримінації, булінгу, цькування та утиску прав здобувачів освіти.

**Відвідування занять та участь в них**

Навчання побудоване на застосуванні активних методів навчання. Активна участь є очікуванням і нормою.
Відвідуваність та активна участь складають 80% від оцінки.
Студент, який з поважних причин, підтверджених документально, не підлягав поточному контролю має право пройти поточний контроль у двотижневий термін після повернення до навчання.

Студент, що був відсутній на заняттях без поважних причин, не брав участі у заходах поточного контролю, не ліквідував академічну заборгованість, не допускається до підсумкового семестрового контролю знань з цієї дисципліни, а в день складання іспиту в екзаменаційній відомості науково-педагогічним працівником виставляється оцінка «недопущений». Повторне складання іспиту з дисципліни призначається за умови виконання всіх видів навчальної, самостійної (індивідуальної) роботи, передбачених робочою навчальною програмою дисципліни, і проводиться згідно із затвердженим директоратом графіком ліквідації.

**Академічна доброчесність**

Цілісність академічної діяльності будь-якого закладу вищої освіти вимагає чесності в навчанні та дослідженнях, тому академічна доброчесність вимагається від усіх студентів МЄУ. Академічна недоброчесність заборонена в усіх програмах нашого університету. Всі учасники освітнього процесу керуються принципами академічної доброчесності.

**Виконання завдання з запізненням, виправлення оцінок, відпрацювання**

Звіти з виконаних завдань мають бути завантажені на Moodle до термінів завершення, зазначених у розкладі курсу. Найкращою практикою буде виконувати завдання якомога швидше після отримання, щоб було достатньо часу для активної участі на заняттях.
Якщо потрібно більше часу для виконання завдання, доступні гнучкі терміни. Виконані завдання приймаються до повного заліку до останнього заняття з дисципліни за розкладом, після чого 40% частковий кредит на основі отриманої оцінки буде нараховано протягом тижня після останнього дня занять. Завдання, які взагалі не здавалися, отримають 0.
Якщо заняття пропущені більше ніж на один тиждень через хворобу або з інших причин, необхідно зв'язатися з викладачем, щоб домовитися про альтернативні варіанти виконання завдань. Дедлайни працюють в обидві сторони, і їх дотримання гарантує, що викладачем буде наданий своєчасний зворотний зв’язок щодо ваших завдань, щоб переконатися, що ви не відстаєте від курсу.

**Час відповіді викладача (про перевірку завдань)**

Через корпоративну пошту (впродовж 24 годин), через меседжери (протягом 1-2 годин)

**Ефективна комунікація**

Ефективна комунікація має важливе значення для успіху в цьому курсі, рекомендуємо використовувати такі канали:

- *Форум запитань і відповідей*: щоб отримати загальні запитання курсу, необхідно перевірити розділ F.A.Q у Moodle, а потім опублікувати своє запитання на форумі запитань і відповідей, щоб поставити його своїм колегам або ж викладачу (гарантоване отримування сповіщення

електронною поштою щоразу, коли з'являється нова публікація чи відповідь на поставлене запитання);

- *Електронна пошта*: маєте особисте запитання, пов'язане з вивченням курсу, напишіть викладачу безпосередньо;
- *Соціальні мережі, меседжери*: особиста комунікація із одногрупниками, викладачем;
- *Очна зустріч:* комунікація з одногрупниками під час проведення занять та з викладачем у консультаційні дні.

**Політика щодо ChatGPT та іншого генеративного ШІ**

Використання генеративного ШІ дозволяється.

**Використання електронних пристроїв на заняттях**

Електронні пристрої (смартфон, планшет, лаптоп) дозволяється використовувати лише для цілей, пов'язаних із заняттями, а також якщо вони потрібні, щоб зробити вміст курсу доступним.
Смартфон повнен бути переведений у беззвучний режим підчас заняття. Якщо є серйозні обставини, такі як надзвичайна ситуація в сім'ї, через яку, можливо, доведеться відповісти на телефонний дзвінок, необхідно повідомити викладача про це до початку заняття, щоб можна було тихо вийти з аудиторії та відповісти на дзвінок.
Крім того, жодна частина заняття не може бути записана аудіо чи відео без згоди викладача та згоди одногрупників. Це порушує конфіденційність інших студентів і може перешкоджати участі інших студентів і заважати їхньому навчанню.

**Політика публікації та розповсюдження матеріалів курсу**

Студенти не можуть розміщувати, публікувати, продавати або іншим чином публічно поширювати матеріали курсу без письмового дозволу викладача.
Такі матеріали включають: конспекти лекцій, слайди (презентації) лекцій, відео чи аудіозаписи, завдання, набори задач, тести, роботи інших студентів і відповіді та ін.
Студенти, які продають, розміщують, публікують або розповсюджують матеріали курсу без письмового дозволу чи іншим чином, можуть бути притягнуті до дисциплінарної відповідальності, аж до вимоги відмовитися від навчання.

# Очікуване навантаження та залученість студентів

На роботу в цьому курсі слід виділити приблизно 4 годин на тиждень. Якщо виникнуть обставини, що змушують витратити більше часу на якесь з завдань, необхідно проінформувати викладача електронною поштою (меседжером). Продовження терміну здачі можливо лише за умови, що викладач попередньо проінформований про те, що неможлива здача

завдання до зазначеного часу. Очікується, що студенти мають резервний план на випадок несправності комп'ютера або перебоїв у роботі Інтернету.

# Служби підтримки

Електронний розклад: https://rozklad.ieu.edu.ua
Онлайн бібліотека: https://onlinelibrary.ieu.edu.ua
Репозитарій: https://sed.ieu.edu.ua/index.php/sed/index
**Освітній Омбудсмен:** https://ieu.edu.ua/pro-mieu/ombudsmen

# Розклад курсу

| Назва теми | Зміст практичного/семінарського заняття |
|---|---|
| *Тема 1.* Основні поняття безпеки програм та даних. Основні принципи захисту програмного забезпечення. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №1*. Логування дій користувачів у програмних системах;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника |
| *Тема 2.* Ідентифікація та автентифікація користувачів. Системи аналізу захищеності мережі. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №2*. Розробка програми розмежування повноважень користувачів на основі парольного аунтифікації;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 3.* Методи та засоби обмеження доступу до програм та даних. Захист програм від несанкціонованого дослідження. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №3*. Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 4.* Криптографічний захист інформації. Віртуальні приватні мережі. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №4*. Формування вмінь і навиків реалізації Blockchain;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 5.* Механізми шифрування. Симетричні та несиметричні криптосистеми. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №5:* Інструменти створення віртуальних приватних мереж;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 6.* Основи технології відкритих ключів (PKI). | ▪ *Контроль на лекції*;<br>▪ *Практична робота №6*. Використання хеш-функцій (на прикладі MD5), оцінка стійкості паролю до зламу; |

| | |
|---|---|
| | ▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 7.* Основи цифрової стенографії. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №7*. Електронний цифровий підпис на прикладі GnuPG для захисту документів та електронної пошти;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 8.* Основи криптоаналізу | ▪ *Контроль на лекції*;<br>▪ *Практична робота №8*. Методи приховування інформації в потоках даних;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 9.* Основні принципи захисту програмного забезпечення. Захист програмного забезпечення в Інтернет-технологіях. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №9*. Алгоритми та методи шифрування в комп'ютерних системах;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 10.* Захист персональних даних. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №10.* Інструментальні засоби захисту програм та даних;<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |
| *Тема 11.* Комплексні системи захисту іноформації. | ▪ *Контроль на лекції*;<br>▪ *Практична робота №11*. Розробка політики конфіденційності IT-компанії відповідно до вимог GDPR;<br>▪ *Практична робота №12*. Створення DMZ (demilitarized zone) для IT-компанії з урахуванням питань безпеки даних<br>▪ *Виконання індивідуальної роботи*. Створення тлумачного словника. |

# Поради щодо успішного навчання

Якщо Ви бажаєте успішно засвоїти цей предмет, необхідно бути:

- наполегливим, уважним і допитливим;
- креативним і життєрадісним, відкритим для спілкування та дискусій;
- готовим отримувати інформацію і знання з предмету не лише на лекціях, а й у позаурочний час.