



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптологія

Рівень вищої освіти	Другий (магістерський)
Код та назва спеціальності, галузь знань	F5 Кібербезпека та захист інформації; F Інформаційні технології
Тип та назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-8)
Курс, семестр викладання	1 курс, 1 семестр
Трудовість навчальної дисципліни	4 кредити ЄКТС (120 академічних годин), з них: денна (очна) форма навчання: лекц. – 20 год., лаб.зан. – 12 год., практ. зан. – 12 год., самост. роб. – 76 год.; заочна форма навчання: лекц. – 10 год., лаб.зан. – 6 год., практ. зан. – 6 год., самост. роб. – 98 год
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладачі

БАСОВ Віктор Євгенович



Старший викладач кафедри «Кібербезпеки та технічного захисту інформації»
Кандидат технічних наук
E-mail: v.y_basov@suitt.edu.ua
Консультації: щосередини з 14²⁰ до 15⁴⁰ год., каб. 205 (головний корпус)

ВАСІЛІУ Євген Вікторович



Професор кафедри «Кібербезпеки та технічного захисту інформації»
Доктор технічних наук
E-mail: y.v_vasiliu@suitt.edu.ua
Консультації: щоп'ятниці з 14²⁰ до 15⁴⁰ год., каб. 205 (головний корпус)

Мета дисципліни	– формування системних знань та розвиток умінь щодо експлуатації, аналізу та розробки криптографічних систем захисту інформації при її створенні, зберіганні та передаванні через не захищене середовище.
Компетентності, формуванню яких сприяє дисципліна	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. СК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. СК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
Програмні результати навчання	ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які

стосуються інформаційної безпеки та/або кібербезпеки.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Програма навчальної дисципліни

Тема 1. Технологія розрахунків над еліптичними кривими в полях Галуа.

Алгебраїчні розрахунки над еліптичними кривими. Повна та скорочена форма Вейєрштраса запису рівняння еліптичної кривої. Будьяка пряма перетинає еліптичну криву у трьох точках. Поняття нескінченно віддаленої точки. Сума трьох точок кривої, що належать одній перетинаючій прямій. Чому дорівнює сума двох крапок Додавання та подвоєння точки. Дискретна еліптична крива в полі Галуа. Особливі та неособливі дискретні еліптичні криві.

Тема 2. Двоключові криптосистеми над еліптичною кривою.

Двоключовий алгоритм створення сеансового ключа Опис алгоритму та приклад розрахунку. Двоключовий алгоритм шифрування над еліптичною кривою. Опис алгоритму та приклад розрахунку. Двоключовий алгоритм цифрового підпису над еліптичною кривою. Опис алгоритму та приклад розрахунку. Стандартизація та сучасні практики застосування криптографічних алгоритмів.

Тема 3. Криптоаналіз поточних шифрів

Регістри зсуву з лінійним (РЗЛЗЗ) та нелінійним (РЗНЗЗ) зворотнім зв'язком, причина непридатності для шифрування регістрів з нелінійним зворотнім зв'язком, зв'язок довжини регістру з максимальною довжиною послідовності, що не повторюється, поняття лінійної складності. Примітивний пов'язаний з регістром багаточлен – необхідна умова генерації послідовності максимальної довжини. Яку довжину послідовності слід перехопити, щоб зламати шифр на ґрунті РЗЛЗЗ. Побудова системи лінійних рівнянь та рішення системи – спосіб зламати шифр на ґрунті РЗЛЗЗ.

Тема 4. Криптоаналіз двоключових криптосистем за допомогою факторизації

Особливості обрання параметрів двоключової криптосистеми, які впливають на стійкість. Поняття сильних простих чисел, та первообразних коренів у полях Галуа. Функція Ейлера як секретний параметр криптосистеми. Вплив цих характеристик на криптостійкість. Приклади атак на не стійку реалізацію алгоритму RSA. Атака на ключ RSA та методи факторизації: повний перебор, Р-1 метод Полларда, ро метод Полларда, лямда метод Полларда, метод решета у числовому полі, відомості про квантовий алгоритм Шора. Приклади розрахунку в таких атаках та оцінювання складності атаки.

Тема 5. Криптоаналіз двоключових криптосистем за допомогою дискретного

Особливості обрання параметрів двоключові криптосистеми, які впливають на стійкість. Поняття сильних простих чисел, та первообразних коренів у полях Галуа. Метод Поліга-Хеллмана як універсальний метод пошуку дискретних логарифмів. Вплив цих характеристик на криптостійкість. Приклади атак на не стійку реалізацію алгоритму Діффі-Хеллмана. Атака на ключ RSA та методи пошуку дискретного логарифму: повний перебор, «кроки немовля – кроки велетня», ро метод Полларда, лямда метод Полларда, відомості про квантовий алгоритм Шора. Приклади розрахунку в таких атаках та оцінювання складності атаки. Дискретне логарифмування над еліптичною кривою та атака на шифр методом «кроки

<i>логарифмування</i>	немовля – кроки велетня».
Тема 6 <i>Диференціальний криптоаналіз симетричних шифрів</i>	Загальна схема атаки на симетричний шифр. Поняття диференціалу, методик розрахунку диференціалів, приклад диференціального криптоаналізу одного етапу шифру DES та трьох етапів.
Тема 7 Лінійний криптоаналіз симетричних шифрів	Загальна схема атаки на симетричний шифр. Поняття ефективного лінійного статистичного аналогу нелінійних перетворень, приклад лінійного криптоаналізу одного етапу шифру DES та чотирьох етапів.
Тема 8 Лінійно-диференціальний криптоаналіз симетричних шифрів	Загальна схема атаки на симетричний шифр. Методика комбінування лінійного та диференціального криптоаналізу. Приклад лінійно-диференціального криптоаналізу на 7 та 8 етапів шифру DES.
Тема 9 Криптоаналіз слайдова атака	Загальна схема атаки на симетричний шифр. Методика криптоаналізу слайдова атака. Приклад криптоаналізу слайдова атака зі зсувом на 1 та 2 етапи шифру DES.
Тема 10 Квантовий криптоаналіз та постквантова криптографія	Алгоритми криптоаналізу за допомогою квантових комп'ютерів. Алгоритми постквантової криптографії.

Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання:

Інтерактивні	- Наочно-демонстраційні дидактичні комплекси до тем, що вивчаються в межах дисципліни (схеми, таблиці, графіки, діаграми; зображення, картини, зарисовки, фотографії; відеоролики; стрічки новин чи подій; гіфки, меми; комікси; квести, кросворди, ребуси тощо). - Відповіді на запитання і опитування думок здобувачів освіти (дискусії). - Відпрацювання навичок та робота в групах. Організовується групова робота (2–6 осіб) із конкретними завданнями, що виконуються спільно з взаємодопомогою, після чого результати презентуються в аудиторії для розвитку професійних і командних навичок.
Практичні	Вправи. Різні практичні завдання, які застосовуються на будь-якому етапі навчального процесу і допомагають

**Методи
дистанційного
навчання**

- здійювати інтелектуальні, комунікативні та пошукові здібності здобувачів освіти. Вони можуть включати відповіді на запитання, розв'язання задач, виправлення помилок, складання порівняльних таблиць, графіків і т.п.
- Творчі роботи (проекти). Мета таких робіт – розвиток творчого мислення, підвищення технічних навичок роботи з необхідним програмним забезпеченням та обладнанням.
 - Відеоконференції в форматі лекцій або семінарів. Зв'язок здобувачів освіти з викладачем забезпечують різноманітні сучасні платформи, такі як: Zoom, Moodle, Google Meet та ін.
 - Онлайн дискусії;
 - Індивідуальне і групове консультування (викладач дає додаткові роз'яснення щодо виконання завдань через чати та e-mail-надсилання);

Стратегія оцінювання результатів навчання

**Змістовий контент
результатів
навчання з
дисципліни**

Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 7 рівня Національної рамки кваліфікацій, що відповідає другому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме:

- **Знання** – очікується засвоєння основних концепцій, принципів і методів сучасної криптології, математичних основ криптографії, принципів побудови та функціонування симетричних і асиметричних криптосистем, криптографічних протоколів, а також основних методів криптоаналізу та оцінювання криптографічної стійкості.
- **Уміння/навички** – формується здатність застосовувати математичні методи для аналізу криптографічних алгоритмів і систем, виконувати розрахунки параметрів криптосистем, досліджувати їх криптографічну стійкість, застосовувати методи криптоаналізу симетричних та асиметричних криптосистем, оцінювати складність криптоаналітичних атак, а також аналізувати сучасні підходи до квантового криптоаналізу та постквантової криптографії.
- **Комунікація** – здатність аргументовано представляти та обговорювати результати дослідження криптографічних систем і методів криптоаналізу, пояснювати принципи роботи криптографічних алгоритмів, обґрунтовувати вибір криптографічних методів і засобів та взаємодіяти з фахівцями під час вирішення професійних завдань у сфері інформаційної безпеки та кібербезпеки.
- **Відповідальність і автономія** – здатність самостійно аналізувати криптографічні системи, оцінювати їх стійкість до відомих методів атак, обґрунтовувати вибір криптографічних алгоритмів і параметрів відповідно до поставлених завдань та самостійно розв'язувати складні нестандартні задачі у сфері криптографічного захисту інформації.

Критерії оцінювання

Академічні успіхи здобувачів освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов'язковим переведенням кількості балів в оцінки за національною

шкалою та за шкалою ECTS.

Відмінно (A) – від 90 до 100 балів – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі або не менше 90% завдань, передбачених програмою навчальної дисципліни.

Дуже добре (B) – від 82 до 89 балів – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішив 80-89% письмових завдань.

Добре (C) – від 74 до 81 балів – здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив 74-81% письмових завдань.

Задовільно (D) – від 64 до 73 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішив 64-73% письмових завдань.

Задовільно (E) – від 60 до 63 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив 60-63% письмових завдань.

Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів – здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив 35-59% письмових завдань.

Незадовільно з обов'язковим повторним вивченням дисципліни (F) – від 0 до 34 балів – Здобувач частково володіє навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив 1-34% письмових завдань.

Форма та методи контролю начальних досягнень	В межах даної дисципліни передбачено три види контролю: поточний, підсумковий та семестровий. Поточний контроль здійснюється під час проведення лекційних, лабораторних та практичних занять і має на меті перевірку рівня підготовленості здобувачів до виконання конкретної роботи з теми, що вивчається. При поточному контролі оцінюється: активність роботи здобувача на заняттях, результати виконання лабораторних та практичних робіт, індивідуальних завдань і контрольних робіт, якість виконання завдань під час самостійної роботи. Формами проведення поточного контролю є тестування, опитування, перевірка та захист лабораторних і практичних робіт. Підсумковий контроль – це накопичена здобувачем сума балів за результатами вивчення навчальних тем та виконання завдань самостійної роботи. Семестровий контроль передбачає проведення екзамену, під час якого здобувачу виставляється остаточна оцінка за навчальну дисципліну відповідно до чинної в ДУІТЗ системи оцінювання.
	Політика навчальної дисципліни
Відвідування	Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен) є обов’язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.
Дотримання принципів академічної доброчесності	Здобувачі вищої освіти зобов’язані дотримуватися принципів академічної доброчесності відповідно до чинного законодавства та внутрішніх нормативних документів ДУІТЗ. Навчальні та індивідуальні завдання виконуються самостійно, з обов’язковим посиланням на використані джерела. Не допускаються плагіат, списування, фабрикація, фальсифікація та інші порушення академічної доброчесності. У разі використання матеріалів, створених із застосуванням технологій штучного інтелекту, факт такого використання зазначається відповідно до встановлених вимог. Викладач має право для перевірки робіт застосовувати різні програмні засоби.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.
Інші умови	Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.

Рекомендовані джерела інформації

Базові підручники та навчальні посібники

1. Smart Nigel Cryptography: An Introduction, 3rd Edition.—A McGraw Hill Publication., 2003Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
2. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p.
3. І.В. Самойлов, А.А. Матійко, А.С. Сторчак Криптографія [Навч. посіб.] Рік видання 2023 — КПІ. 125 «Кибербезпека»
4. Сагун А.В., Хайдуров В.В., Нікітенко Є.В., Мамченко С.М. Основи криптоаналізу. Навч. посіб. Рік видання 2024 – Київ, Ін-т загальної енергетики НАН України
5. ДСТУ ISO/IEC 9798.
6. ДСТУ ISO/IEC 15946.
7. Рекомендації X.800

Методичні рекомендації та розробки викладачів дисципліни

1. Басов В. Є. Криптоаналіз сучасних криптосистем: методичні вказівки до лабор. занять. Рік видання 2025 — ДУІТЗ. 125 «Кибербезпека»
2. Методи та засоби захисту інформації: навч. посібник / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К.: ЦП «Компринт» О.В., 2021. – 444 с.
3. Лімарь І.В. Основи квантової та постквантової криптографії: методичні вказівки до викон. практич. робіт. Рік видання 2025 — ДУІТЗ. 125 «Кибербезпека»

Інформаційні ресурси

<https://ela.kpi.ua/handle/123456789/81461>
<https://www.nist.gov/pqc>
<https://www.nccoe.nist.gov/applied-cryptography>

Рік введення силабусу – 2026 р.

Затверджено рішенням кафедри Кибербезпеки та технічного захисту інформації
(Протокол від 22 травня 2026 р. № 13)

Завідувач кафедри – д.т.н, проф.

Гарант освітньої програми к.т.н. доц.

Старший викладач, к.т.н.:

Професор, д.т.н.



Володимир КОРЧИНСЬКИЙ

Віталій КІЛЬДІШЕВ

Віктор БАСОВ

Євген ВАСІЛІУ