КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ОПИС КУРСУ

Криптографічні методи захисту інформації – це курс зосереджений на формуванні теоретичних знань і практичних навичок у сфері захисту даних із використанням сучасних криптографічних методів і протоколів. Програма курсу охоплює повний цикл розвитку криптографії – від історичних шифрів до сучасних алгоритмів, мережевих протоколів і постквантових рішень, що застосовуються в інформаційних системах, мережах та програмному забезпеченні.

У межах курсу студенти ознайомляться з фундаментальними поняттями криптографії, цілями захисту інформації та загрозами інформаційній безпеці. Значна увага приділяється симетричним і асиметричним алгоритмам шифрування, принципам блочного шифрування, хеш-функціям, цифровим підписам і механізмам управління криптографічними ключами. Розглядаються традиційні та сучасні стандарти, а також практичні аспекти їх використання в реальних системах.

Курс також охоплює методи захисту інформації на рівні мережевих протоколів (TLS, SSH, VPN), механізми аутентифікації та верифікації користувачів, а також аналіз типових криптографічних атак і способів протидії їм. Окремий розділ присвячено постквантовій криптографії та підготовці інформаційних систем до викликів, пов'язаних із розвитком квантових обчислень.

У результаті вивчення курсу студенти отримають комплексне розуміння сучасних криптографічних підходів, навчаться коректно обирати та застосовувати алгоритми й протоколи захисту інформації, оцінювати їхню стійкість і безпеку, а також будувати надійні системи захисту даних у практичних IT-проєктах.

ВИМОГИ

–базові знання програмування (бажано на мові C#);

–базові навички використання IDE;

–наявність корпоративного облікового запису @mipolytech.education, Microsoft Teams, Word;

–наявність особистого логіну та паролю в Moodle (для отримання або поновлення слід звернутися до відповідальної особи на факультеті).

Освітній рівень	Бакалавр
Кількість кредитів	5,0
Назва кафедри, яка пропонує дисципліну	Цифрових технологій та проєктно-аналітичних рішень

КАСЬЯНЮК Олександр

oleksandr.kasianiuk@mipolytech.education

старший викладач кафедри ЦТПАР,

Професійні інтереси: розробка програмних додатків на C# у .Net; програмування мобільних додатків на C#; програмування мікроконтролерів та IoT; генеративний штучний інтелект; low-code автоматизація

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

- знання базових алгоритмів захисту інформації;
- представлення про світові та державні стандарти захисту інформації;
- розуміння методів та підходів до захисту інформації;
- знання про цифрові сертифікати, підписи та методи верифікації, авторизації та автентифікації.

ТЕМАТИКА

Вступ до криптографії. Давні шифри криптографії. Принципи блочного шифрування та Спрощений DES. Традиційні алгоритми блочного шифрування. Хешування даних. Криптографічний захист інформації. Цифрові підписи. Мережеві криптографічні протоколи. Аутентифікація та верифікація користувача. Криптографічні атаки. Постквантова криптографія

ОРГАНІЗАЦІЯ КУРСУ, ФОРМИ ТА МЕТОДИ НАВЧАННЯ

- освітній процес будується як комбінація лекцій та самостійного вивчення навчального матеріалу на платформі Moodle – з одного боку, та практичних занять з відпрацювання теоретичного матеріалу на практичних прикладах – з іншого.
- відвідування лекційних занять є бажаним, однак не обов'язковим; від студентів очікується ознайомлення з матеріалом перед лекцією, що дозволить побудувати лекційне заняття у вигляді сполучення пояснень викладача та обговорення проблемних питань, які виникли при підготовці до лекції.
- практичні заняття передбачають опанування теоретичного матеріалу на практичних прикладах; їх відвідування є бажаним.
- від студента потребується виконати індивідуальні завдання та модульні контрольні роботи у терміни, встановлені у розділі «Розподіл балів за контрольними точками та графік їх виконання».
- з урахуванням поточної ситуації від учасників освітнього процесу очікується виконання вимог безпеки при сигналі «Повітряна тривога», санкції за залишення заняття або неявку на заняття не застосовуються.
- опціонально доступні індивідуальні та групові консультації. З викладачем можна зв'язатися через електронну пошту, в чаті або в персональній розмові в MS Teams.

ПІДХОДИ ДО ОЦІНЮВАННЯ

Розподіл балів за контрольними точками та графік їх виконання

Тижні / Види контр. точок	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Всього
Робота на практичних заняттях			6		8		6					6		7		7			40
Складання індивідуальних завдань								20									20		40
Модульні контрольні роботи									10									10	20
Всього	50									50									100

Зміст та вимоги до контрольних точок

Назва контрольної точки	Опис контрольної точки, порядок її проходження та отримання балів
Робота на практичних заняттях	Оцінка за роботу на практичному занятті оголошується після демонстрації звіту про виконану роботу у вигляді файлу *docx, або *pdf розміщується у відповідному розділі дисципліни в Moodle. Максимальна оцінка встановлена для кожної практичної роботи окремо, але 2 бали з них студент отримує за захист цієї роботи.
Виконання та захист індивідуального завдання	Підготовлений звіт у вигляді файлу *docx, або *pdf розміщується у відповідному розділі дисципліни в Moodle і перевіряється протягом тижня після завершення терміну подачі. Оскарження оцінки може бути здійснене на останньому практичному занятті модуля. Максимальна 20 балів: – студент підготував звіт в якому ретельно описав свої дії та зробив висновки по роботі у науковому стилі (5 балів); – робота містить чітке виконання всіх пунктів індивідуального завдання, які прописані у відповідному файлі з завданням (10 балів); – студент під час презентації / захисту роботи демонструє володіння термінологічним апаратом, відповідає на запитання (5 бали)
Модульні контрольні роботи	МКР виконуються в Moodle під час останнього практичного заняття в модулі за 1 годину 10 хвилин. В разі неявки або неможливості виконання МКР з поважних причин на таке заняття допускається відкриття виконання МКР за погодженням з викладачем в інший час асинхронно. Кількість спроб не обмежується, однак обмеження по часу виконання МКР залишається. Кожна модульна контрольна робота включає відкриті питання з матеріалу модуля (max 10 балів).

Додаткові зауваження:

– студент може оскаржити отримані оцінки в порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи : Polytechnic (metinvest.university))та Положенням про політику та процедури врегулювання конфліктних ситуацій (Академічні політики : Polytechnic (metinvest.university))

– оцінки, отримані за роботу на практичних заняттях не можуть бути відпрацьовані або покращені, окрім процедури оскарження, оцінки за інші види поточного контролю можуть бути покращені за індивідуальною домовленістю з викладачем;

– викладач не має права знижувати оцінку за індивідуальне завдання або модульну контрольну роботу, якщо вони не були складені вчасно, однак в разі, якщо така робота була оцінена пізніше, ніж момент завершення теоретичного навчання у семестрі, то відповідна оцінка не враховується у рейтингу здобувачів освіти.

Форма підсумкового контролю. Порядок визначення підсумкової оцінки

Форма підсумкового контролю	Залік, тобто підсумкова оцінка вставляється як сума оцінок поточного контролю без проведення додаткових контрольних заходів
Умови допуску до підсумкового контролю	якщо сума оцінок за поточний контроль за семестр становить менше 60 балів, необхідно відпрацювати відповідні види контролю поточної успішності до звершення теоретичного навчання
Порядок визначення підсумкової оцінк	Для варіанту заліку: - якщо протягом семестру за результатами поточного контролю здобувач освіти набрав менше 60 балів, то під час екзаменаційної сесії йому надається змога отримати/покращити власний результат з усіх видів поточного контролю, крім активності на навчальних заняттях; - в разі, якщо протягом семестру за результатами поточного контролю або в процесі покращення власних результатів здобувач освіти набрав більше 60 балів, йому виставляється фактична сума балів і оцінка «залік», в іншому випадку – «незалік».

Відповідність між прийнятими в університеті шкалами оцінки наведена в таблиці

Бальна шкала	Рівні	Характеристика	Традиційні шкали	
			Іспит	Залік
90-100	A	Студент демонструє видатний рівень досягнення запланованих результатів вивчення навчальної дисципліни, що засвідчують його безумовну готовність до подальшого навчання та/або професійної діяльності за фахом	Відмінно	Залік
82-89	B	Студент виявляє вищий за середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні незначні помилки	Добре	
75-81	C	Студент виявляє середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні деякі значущі помилки		
67-74	D	Студент виявляє задовільний рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях наявні суттєві помилки	Задовільно	
60-66	E	Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати вивчення навчальної дисципліни		
35-59	FX	Низка запланованих результатів навчання не досягнуті. Рівень наявних результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом	Незадовільно	Незалік
0-34	F	Результати навчання відсутні або критично низькі		

ОСОБЛИВІ ПІДХОДИ ДО ВИЗНАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

– В разі, якщо дисципліна є обов'язковою для здобувача освіти, і він засвоїв повністю або частково відповідні програмні результати навчання під час отримання освіти на попередніх або такому ж рівні, то кредити та оцінка з дисципліни може бути перезарахована в порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи : Polytechnic (metinvest.university)). Консультацію з даного питання можна отримати у викладача, куратора або гаранта освітньої програми, завідувача кафедри, за якою закріплено цю дисципліну;

– В разі, якщо здобувач освіти обрав цю дисципліну як дисципліну вільного вибору, не зважаючи на той факт, чи вивчалася вона раніше, оцінка та кредити з цієї дисципліни не перезараховуються;

– В разі, якщо здобувач освіти хотів би самостійно вивчити певні курси за тематикою цього курсу (наприклад, Coursera, Udemy або інших платформ, в т.ч. платформ відкритих курсів вітчизняних та/або закордонних університетів), то 1) доцільно звернутися до списку рекомендованих вебресурсів або проконсультуватися з викладачем на предмет релевантності самосійтно знайденого освітнього ресурсу програмі дисципліни; 2) в разі успішності опанування такого курсу, яке підтверджується сертифікатом або іншим способом, такому здобувачу у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи : Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного контролю;

– В разі, якщо здобувач освіти реалізував певний вид наукової роботи (тези, стаття, результативна участь у студентській олімпіаді тощо), то у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи : Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного або навіть підсумкового контролю; перелік таких осіб можна знайти за посиланням Студентам : Polytechnic (metinvest.university)

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Easttom C. Modern cryptography : applied mathematics for encryption and information security. 2nd ed. Cham : Springer Nature, 2022. ISBN 978-3-031-12304-7. URL: https://read.kortext.com/library/books/2087649
2. Utzke D. The digital asset technology guidebook : deciphering the keys to crypto, blockchain, and decentralized finance. 1st ed. Hoboken : Wiley, 2025. 255 p. ISBN 978-1-394-31960-2. URL: https://read.kortext.com/library/books/3757793
3. Musa S. M. Network security and cryptography. 2nd ed. Birmingham : Packt Publishing, 2024. 611 p. ISBN 978-1-83664-156-8. URL: https://read.kortext.com/library/books/3033494

АКАДЕМІЧНІ ПОЛІТИКИ

Як член спільноти Технічного університету «МЕТІНВЕСТ ПОЛІТЕХНІКА» Ви маєте дотримуватися певних стандартів та академічної політики:

– ***Академічна недоброчесність*** вигляді академічного плагіату; фабрикації; фальсифікації; списування обману; хабарництва; необ'єктивного оцінювання; надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання – прямо заборонено (докладніше про це – у Положенні про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ТОВ ТЕХНІЧНОГО УНІВЕРСИТЕТУ «МЕТІНВЕСТ ПОЛІТЕХНІКА»); і в разі виявлення – ***відповідний захід контролю (контрольну точку) буде оцінено в 0 балів за з наступним повідомленням декану факультету та голові комісії з академічної доброчесності Університету***.

– В разі випадку надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання студент може оскаржити процедури оцінювання за процедурами, передбаченими Положенням про організацію освітнього процесу (розділ 10).

– Матеріали в рамках курсу, захищені авторським правом, можуть бути використані лише тільки здобувачами освіти, яким призначено даний курс і для цілей, пов'язаних з цим курсом і не можуть поширюватися.

– Спілкування з однокурсниками та викладачем має бути професійним та ввічливим.

– Очікується, що Ви перевірятимете всі Ваші письмові повідомлення, включаючи поштові повідомлення та повідомлення у MS Teams на коректність змісту та мови.

– Університет прагне підтримувати середовище, вільне від дискримінації або дискримінаційних домагань, спрямованих на будь-яку людину або групу в межах своєї спільноти - здобувачів освіти, співробітників або відвідувачів.

Докладніше про академічні політики стосовно етичності поведінки, академічної доброчесності та протидію булінгу можна дізнатися за посиланням: Академічні політики - Polytechnic (metinvest.university)