СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційни технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-22 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Басов Віктор Євгенович
basvic@bigmir.net

Старший викладач кафедри «Кібербезпеки та технічного захисту інформації»
Кандидат технічних наук за фахом 05.12.02 – Телекомунікаційні системи та мережі

Онацький Олексій Віталійович
onatsky@meta.ua

Доцент кафедри кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Криптографічний захист інформації» об’єднує та узагальнює такі дисципліни, як криптографія, криптографічні протоколи та криптоаналіз. Вона інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: дискретна математика, теорія ймовірностей та комбінаторика, теорія зв’язку, теорія інформації,

	кодування. Навчання спрямовано на: 1) формування у здобувачів вищої освіти системного уявлення про застосування та розробку криптографічних систем захисту інформації в процесах створення, зберігання та передавання коніфденційної інформації, а також чинників, що впливають на цей процес; 2) розвиток умінь з правильної експлуатації криптографічних систем, аналізу та розробки криптографічних протоколів, навичок оцінювання стійкості криптосистем до криптоаналітичних атак, та атак на криптографічні протоколи; 3) надання базових знань та первинних навичок до криптоаналізу як історичних, так і сучасних криптосистем та криптогафічніх протоколів; 4) аналіз та розробка криптографічних протоколів для розподілу ключів в секретних мережах зв'язку та протоколів розділення секрету.
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	ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. КЗ1. Здатність застосовувати знання у практичних ситуаціях КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням КФ4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Результати навчання	ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

	ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних. ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
Обсяг дисципліни	Загальний обсяг дисципліни: 10 кредитів ЄКТС (300 годин). Для денної форми навчання: У семестрі 3.2 – 3 кредити (90 годин): лекції – 20 годин, практичні заняття –10 години, лабораторні заняття –28 годин, самостійна робота – 32 годин. У семестрі 4.1 – 4 кредити (120 годин): лекції – 14 годин, практичні заняття –10 години, лабораторні заняття – 20 годин, самостійна робота – 76 годин. У семестрі 4.2 – 3 кредити (90 годин): лекції – 12 годин, практичні заняття –10 години, лабораторні заняття – 0 годин, самостійна робота – 68 годин.
Форма підсумкового контролю	У семестрі 3.2 - залік по закінченні вивчення дисципліни. У семестрі 4.1 – екзамен та курсова робота та іспит по закінченні вивчення дисципліни. У семестрі 4.2 - екзамен
Терміни викладання дисципліни	Дисципліна викладається у 6-му 7-му та 8-му семестрі

Програма дисципліни

Криптрогафічний захист інформації (частина 1)

	Змістовий модуль 1. Архітектура систем захисту інформації
Тема 1.	**Актуальність проблеми захисту інформації в сучасних системах телекомунікації.** Основні поняття та визначення. Властивості інформації, що підлягає захисту в комунікаційних системах та мережах. Відкрита та секретна інформації. Принцип рівноміцного захисту. Аналіз погроз інформації при передачі по каналах зв’язку. Засоби захисту інформації при передачі відкритими каналами зв'язку. Поняття криптографії та криптоаналізу. Основи архітектури систем захисту інформації. Умови стійкості шифрів. Класичні методи

	шифрування. Основи дешифрування класичних шифрів.
Тема 2.	**Схема секретної системи зв'язку.** Типи й класифікація алгоритмів шифрування. Вимоги до криптосистем.
Тема 3.	**Блочні алгоритми шифрування.** Шифри на базі мережі Фейстеля. Схема алгоритму шифрування DES. Алгоритм 3-DES. Шифр AES. Стандарт шифрування IDEA.
Тема 4.	**Стандарт шифрування Калина.** Схема алгоритму шифрування та режими роботи стандарту. Порівняльний аналіз симетричних криптосистем
Змістовий модуль 2 . Асиметричні криптосистеми захисту інформації	
Тема 5.	**Принципи керування ключовою системою.** Генерування, зберігання та розподілення ключів. Прямий обмін ключами між користувачами. Метод Діффі-Хеллмана.
Тема 6.	**Криптосистеми з відкритим ключем.** Процедури шифрування в криптосистемі Ель–Гамаля. Шифрування в криптосистемі RSA
Тема 7.	**Системи ідентифікації та автентифікації.** Ідентифікація та автентифікація. Проста автентифікація, що використовує паролі та PIN-коди. Схема автентифікації з використанням пароля. Атаки на фіксовані паролі.
Тема 8.	**Біометрічні методи ідентифікації та автентифікації**. Надійність біометричних методів автентифікації. Багатофакторна автентифікація.
Тема 9.	**Електронний підпис (ЕП).** Загальні положення. Методи побудови схем ЕП. Однонаправлені геш-функції. Алгоритм цифрового підпису RSA. Різновиди ЕП. Недоліки ЕП RSA. Мультиплікативна атака.
Криптрогафічний захист інформації (частина 2)	
Тема 1.	***Сервіси та механізми безпеки. Види криптографічних протоколів*** Актуальність протоколів забезпечення безпеки. Визначення сервісів безпеки. Взаємозв'язок функцій (сервісів) і механізмів безпеки. Розподіл функцій безпеки по рівнях еталонної моделі OSI.
Тема 2.	***Протоколи розподілу секрету*** Класифікація криптографічних протоколів. Основне призначення протоколів розподілу секрету. Схема розподілу секрету Миньотта, Асмута-Блума, Карнина–Гріна–Хеллмана, Блэкли, Шамира.
Тема 3.	***Протоколи перевіряємо розподілу секрету***

	Основне призначення протоколів перевіряємого розподілу секрету. Схеми перевіряємо розділення секрету Фельдмана, Педерсена. Схема розподілу секрету досконала та ідеальна.
Тема 4.	***Протоколи ідентифікації та автентифікації*** Міжнародні стандарти ISO/IEC 9798. Класифікація систем ідентифікації та автентифікації. Протоколи Фиата–Шамира, Окамото, Шнорра, Фейга–Фиата–Шаміра, Brickell–Mccurley, Guillou-Quisquater
Тема 5.	***Протоколи керування криптографічними ключами*** Генерація, зберігання та розподіл ключів. Методи сертифікації відкритих ключів. Протоколи Шамира, MTI, STS, KEA, MQV, Girault, Kerberos, AKEP2
Тема 6.	***Криптографічні протоколи на еліптичних кривих*** Протоколи розподілу ключів на еліптичних кривих ECMQV, ECDH, ECKEP, Мессі-Омура. Схеми Фиата–Шамира та Окамото на еліптичних кривих.
Тема 7.	***Стандарти ДСТУ 4145, ДСТУ ISO/IEC 14888-2:2015*** Вимоги до системи електронного підпису. Структура системи електронного підпису України. Стандарт електронного підпису ДСТУ 4145–2002, алгоритм електронного підпису EC-KCDSA
Криптрогафічний захист інформації (частина 3)	
Тема 1	***Теорія зв'язку в секретних системах*** Визначення кількості інформації в повідомленнях. Статистичні відомості про мову. Поняття ентропії (ненадійності) повідомлень, питома вага кількості інформації на символ, надлишковість повідомлень та її зв'язок зі стійкістю. Відстань єдиності рішення криптограми. Абсолютно стійкий шифр за К. Шенноном. Ланцюги Маркова і їх застосування в криптоаналізі
Тема 2	***Криптоаналіз шифрів перестановки*** Криптоаналіз шифрів подвійної перестановки та трафаретних шифрів за допомогою Марковських ланцюгів
Тема 3	***Криптоаналіз шифрів одноалфавітної підстановки*** Криптоаналіз шифрів Цезаря, Полібія та будь-якої одно алфавітної підстановки
Тема 4	***Криптоаналіз шифрів багато алфавітної підстановки.*** Метод Казізки для криптоаналізу шифрів Гронсфельда, Віжинера та Бофора.
Тема 5	***Криптоаналіз шифрувальної машини «Енігма»*** Роторні шифрувальні машини, які розроблялись і застосовувались в середені 20-го сторіччя. Принципи побудови та експлуатації німецької шифрувальної машини «Енігма». Індекс співпадінь – як критерій що полегшує атаку на «Енігму» Технологія атаки та оцінювання її складності.
Тема 6	***Загальні методи криптоаналізу симетричних шифрів*** Види криптоаналізу: на ґрунті криптогами, криптограми і відкритого тексту, криптограми і обраного відкритого тексту, атака зі словником. Поняття шифру захищенного по розрахункам. Атаки на грунті «парадоксу днів народження», «зустріч посередин»і, «розділяй та перемагай».

Тема 7	***Криптоаналіз поточних шифрів*** Переваги та недоліки регістрів зсуву зі зворотними зв'язками для застосування в криптографії, вимоги до регістру, щоб генерувалась ннеповторювана послідовність максимальної довжини. Лінійна складність, Алгебраїчна атака на шивр на грунті лінійного регістру

Список рекомендованих джерел

1. Асиметричні методи шифрування: Навч. посіб. / Онацький О.В., Йона Л.Г., Шинкарчук Т.М.; за ред. М. В. Захарченка. – Одеса: ОНАЗ ім. О. С. Попова, 2010. – 164 с.
2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво «Форт», 2012. – 880 с.
3. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко, І.Д. Горбенко. – Харків: Видавництво «Форт», 2010. – 608 с.
4. Розвинення криптології та її місце в сучасному суспільстві. Частина І Класичні методи шифрування та дешифрування. Навчальний посібник. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. – Одеса, 2003. – 105 с.
5. Сучасні криптографічні системи. Навчальний посібник. С.М. Горохов, Л.Г. Йона, О.В. Онацький, під керівництвом проф. М.В. Захарченка Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 с.
6. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації» /О. В. Онацький, Л. Г. Йона, Ю. В. Белова; Держ. ун-т інтелект. технологій і зв'язку. – Одеса : Астропринт, 2023. – 252 с.
7. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal – 1949 – Volume: 28, Issue: 4.
8. Smart Nigel Cryptography: An Introduction, 3rd Edition.–A McGraw Hill Publication., 2003
9. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
10. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p.
11. ДСТУ ISO/IEC 9798.
12. ДСТУ ISO/IEC 15946.
13. Рекомендації X.800.

Інформація про консультації

Кожного понеділка у вересні-листопаді 2024 року з 15^{00} до 16^{20} год., дистанційно. Ст. викл. Басов В. Є.

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється
за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов’язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням …….