Національний технічний університет «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Кафедра обчислювальної техніки

ЗАХИСТ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 Комп'ютерна інженерія*
Освітня програма	*Комп'ютерні системи та мережі*
Статус дисципліни	*Обов'язкова (нормативна) компонента ОП, циклу професійної підготовки*
Форма навчання	*очна / заочна*
Рік підготовки, семестр	*4 курс, вісінний*
Обсяг дисципліни	*4,5 кредитів / 135 годин*
Семестровий контроль/ контрольні заходи	*Екзамен*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, професор Писарчук Олексій Олександрович, kga46826@gmail.com.* Лабораторні: *доктор технічних наук, професор Писарчук Олексій Олександрович, agd015979@gmail.com.*
Розміщення курсу	*https://drive.google.com/drive/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d?usp=sharing* *https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg*

- **Програма навчальної дисципліни**

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Дисципліна «Захист інформації в комп'ютерних системах та мережах » *призначена для набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в комп'ютерних системах з метою запобігання несанкціонованому доступи, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.*

Метою вивчення курсу *«Захист інформації в комп'ютерних системах та мережах» є: набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної* безпеки.

Дисципліна забезпечує наступні програмні результати навчання освітньо-професійної програми Комп'ютерні системи та мережі: ЗК2, ЗК8,,ФК1, ФК4, ФК6, ФК7, ФК8, ФК9, ФК13,

ФК16, ФК17, ФК19, ПРН3, ПРН6, ПРН9, ПРН10, ПРН20.

Мета курсу досягається реалізацією часткових завдань:

1. Вивчення основних положень законодавчої база в сфері захисту інформації в комп'ютерних системах: національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування; законодавчі акти та стандарти інших держав у сфері захисту інформації – 1 лекція;

2. Визначення складу, організаційних, технічних та програмно-апаратних засобів комплексної системи захисту корпоративної інформації: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах; модель порушника; методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу) – 2 лекції, 1 лабораторна робота (2 год.);

3. Комп'ютерні віруси та вірусологія: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів; конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів – 2 лекції, 1 лабораторна робота;

4. Кібернетичні загрози комп'ютерним системам та протидія їм: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак; методології, методи і технології протидії кібернетичним атакам; и, метод програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів – 2 лекції, 1 лабораторна робота;

5. Криптографічний захист інформації в комп'ютерних системах: загальні відомості про класичну криптологію, криптографію та криптографічний аналіз; традиційні історичні шифри; алгоритми блочного шифрування; принципи побудови сучасних симетричних криптографічних шифрів та систем; асиметричні криптографічні системи шифрування (сутність та математичні основи; алгоритми та криптографічні системи; технології реалізації та уразливість) – 9 лекцій, 4 лабораторна робота;

6. Методи, методології, технології і засоби аутентифікації та ідентифікації, як елемент захисту інформації в комп'ютерних системах: методи і технології ідентифікації користувачів; електронний цифровий підпис, центри сертифікації електронних ключів – 2 лекції, 1 лабораторна робота.

За результатами вивчення курсу студент повинен знати:

Основні положень законодавчої база в сфері захисту інформації в комп'ютерних системах: національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування; законодавчі акти та стандарти інших держав у сфері захисту інформації.

Склад організаційних, технічних та програмно-апаратних засобів комплексної системи захисту корпоративної інформації: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах; модель порушника; методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу;

Принципи побудови, дії та захисту від комп'ютерних вірусів та основи вірусології: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і

розповсюдження комп'ютерних вірусів; конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів;

Методи, етапи способи та засоби здійснення кібернетичних атак на комп'ютерні системи, методи, засоби і технології протидії їм: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак; методології, методи і технології протидії кібернетичним атакам; и, метод програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів;

Методи, математичні моделі, алгоритми і технології криптографічного захисту інформації в комп'ютерних системах: загальні відомості про класичну криптологію, криптографію та криптографічний аналіз; традиційні історичні шифри; алгоритми блочного шифрування; принципи побудови сучасних симетричних криптографічних шифрів та систем; асиметричні криптографічні системи шифрування (сутність та математичні основи; алгоритми та криптографічні системи; технології реалізації та уразливість);

Методи, методології, технології і засоби аутентифікації та ідентифікації, як елемент захисту інформації в комп'ютерних системах: методи і технології ідентифікації користувачів; електронний цифровий підпис, центри сертифікації електронних ключів.

За результатами вивчення курсу студент повинен вміти:

Застосовувати положення законодавчої база в сфері захисту інформації в комп'ютерних системах;

Розробляти, створювати і впроваджувати комплексні системи захисту корпоративної інформації;

Виявляти і протидіяти комп'ютерним вірусам;

Оцінювати уразливість, виявляти ознаки підготовки та здійснення кібернетичних атак, проектувати створювати та впроваджувати заходи і засоби протидії кібернетичним загрозам;

Здійснювати криптографічний захист інформації в комп'ютерних системах;

Впроваджувати дієві механізми аутентифікації та ідентифікації в комп'ютерних системах.

Матеріали курсу використаються для реалізації практичних питань із захисту інформації в процесі професійної діяльності, а також у реалізації завдань курсового проектування, розробки кваліфікаційних робіт тощо.

***Курс включає** 4,5 кредити (135 годин), з яких 54 години – аудиторної підготовки, 81 година – самостійної роботи студентів.*

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Місце дисципліни в структурно-логічній схемі навчання:

Дисципліна відноситься до обов'язкової (нормативної) компоненти ОП, циклу професійної підготовки і базується на дисциплінах Фізика, Дискретна математика, Теорія електричних кіл та сигналів, Архітектура комп'ютерів, Комп'ютерні мережі, Комп'ютерні системи, Алгоритми та методи обчислень. Дисципліна Захист інформації у комп'ютерних системах викладається на завершальному етапі та спрямовано на формування сукупності компетенцій випускника з комп'ютерної інженерії.

3. Зміст навчальної дисципліни

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

***Тема 1.** Основні положення законодавчої база в сфері захисту інформації в комп'ютерних*

системах.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози.*

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура.*

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси.*

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів.*

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак.*

Тема 7. *Методи і засоби протидії кібернетичним атакам.*

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз.*

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи.*

Тема 10. *Традиційні історичні шифри. Технології реалізації та уразливість.*

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

Тема 11. *Алгоритми блочного шифрування. Математичні та алгоритмічні основи.*

Тема 12. *Алгоритми блочного шифрування. Технології реалізації та уразливість.*

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

Тема 13. *Симетричні шифри та системи. Математичні та алгоритмічні основи.*

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість.

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

Тема 15. *Асиметричні шифри та системи. Математичні та алгоритмічні основи.*

Тема 16. *Асиметричні шифри та системи. Технології реалізації та уразливість.*

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Тема 17. *Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах.*

Тема 18. *Електронний цифровий підпис, методи та засоби.*

4. Навчальні матеріали та ресурси (до 20) Убрать русскоязычные

Список основної літератури:

1. Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015. – 226 с. : іл. https://ela.kpi.ua/handle/123456789/48296

2. Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с https://ela.kpi.ua/handle/123456789/48296

3. Хорошко В.А. Методи й засоби захисту інформації / ВА Хорошко, АА Чекатков - К.: ЮНІОР, 2003. https://ela.kpi.ua/handle/123456789/48296

4. Журановський Н.Ф. Теорія інформації та кодування. Підручник. – К.: Професіонал, 2001 https://ela.kpi.ua/handle/123456789/48296.

*5 Писарчук О.О. **Захист інформації в комп'ютерних системах»**: Навч. посібник . [Електронний ресурс] / Писарчук О.О.–Електронні текстові дані (1 файла: 1,8 Мбайт). – Київ : КПІ ім. Ігоря*

Сікорського, 2020. – 95 с. Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 6 від 31.01.2020 р.) за поданням Вченої ради ФІОТ (протокол № 4 від 25.11.2019 р.) https://ela.kpi.ua/handle/123456789/48296

Список додаткової літератури: :

6. Антонюк А.Ф. Основи захисту інформації в автоматизованих системах. Навчальний посібник. - К.: Академія, 2003.

7. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

8. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. – К.: Вид. Національної академії внут. справ, 2012. – 104 с.

9. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510.

10. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

11. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

12. Дронюк І. М. Технології захисту інформації на матеріальних носіях Монографія. Львів : Видавництво Львівської політехніки, 2017. 200 с

13. Kryptographie in C und C++ / MichaelWelschenbach ; translated by David Kramer.2nd American ed., rev. and enl.

***12 Т**арнавський, Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с*

13 Вітер С.А. Захист облікової інформації та кібербезпека підприємства / С.А. Вітер, І.І. Світлишин // Економіка і суспільство: електронне фахове видання. – 2017. – № 11. – С. 497–502.

14 яхович Г.І. Захист облікової інформації в умовах аутсорсингу із використанням інформаційно-комп'ютерних технологій / Г.І. Ляхович // Бізнес Інформ. – 2017. – № 12. – С. 408–412.

15 Шпак В.А. Організація захисту облікової інформації / В.А. Шпак // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. – 2015. – № 2. – С. 181–187.

16 Хорошко В. О. Математичні моделі інформаційно-комунікаційних систем і мереж щодо захисту інформації на основі теорії варіаційно-градієнтних методів / В. О. Хорошко, Т. В. Майсак, Н. Б. Дахно // Моделювання та інформаційні системи в економіці. - 2015. - № 91. - С. 246-255.

17 Эл Свейгарт. Криптография и взлом шифров на Python / Эл Свейгарт, К.:«ДИАЛЕКТИКА», 2020, 512 с.

Інформаційні ресурси:

18.Навчально-методичний комплекс з дисципліни: Захист інформації в комп'ютерних системах [https://drive.google.com/drive/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d?usp=sharing].

19.Електронний курс на освітній платформі Sikorsky «Захист інформації у комп'ютерних системах», 2022: https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg

20.Нормативні документи з питань технічного захисту інформації [http://195.78.68.84/dsszzi/control/uk/doccatalog/list?currDir=41640].

- **Навчальний контент**

5. Методика опанування навчальної дисципліни (освітнього компонента)

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Тема 1. *Основні положення законодавчої база в сфері захисту інформації в комп'ютерних*

системах:

зміст та задачі дисципліни;

національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування;

законодавчі акти та стандарти інших держав у сфері захисту інформації.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози:*

інформація як об'єкт захисту;

категорії інформації, як об'єкту захисту;

канали витоку корпоративної інформації;

загрози інформації в комп'ютерних системах;

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура:*

модель порушника;

методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу).

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси:*

класифікація вірусів;

алгоритми функціонування вірусів;

технології та засоби створення і розповсюдження комп'ютерних вірусів.

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів:*

конструктори вірусів;

антивірусне програмне забезпечення та сутність його побудови і застосування;

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак:*

кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів;

методи і технології організації та реалізації кібернетичних атак.

Тема 7. *Методи і засоби протидії кібернетичним атакам:*

методології, методи і технології протидії кібернетичним атакам (методи, програмне забезпечення та сутність його побудови і застосування);

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз:*

Загальні відомості про шифрування, кодування, криптографію і криптологію;

Задачі дешифрування;

Технології та системи криптографічного захисту інформації.

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи:*

Загальні відомості та галузі застосування.

Шифрування на основі одно та багато алфавітних підстановок: шифри Цезаря та «скитала»;

Шифр Віжинера та квадрати Уітстона.

Біграмні шифри.

Потокові шифри з необмеженою довжиною ключа.

Шифрування «гамуванням».

***Тема 10.** Традиційні історичні шифри. Технології реалізації та уразливість:*

Реалізація традиційних історичних шифрів з використанням засобів Python;

Приклади реалізації традиційних шифрів в Python;

Уразливість традиційних історичних шифрів.

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

***Тема 11.** Алгоритми блочного шифрування. Математичні та алгоритмічні основи:*

Сутність та математичні основи методів блочного шифрування.;

***Тема 12.** Алгоритми блочного шифрування. Технології реалізації та уразливість:*

Технології блочного шифрування в Python, уразливість.

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

***Тема 13.** Симетричні шифри та системи. Математичні та алгоритмічні основи:*

Шифрування на основі чередування перестановок та підстановок;

Стандарт шифрування Data Encryption Standard. (DES).

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість:

Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.

Технології асиметричного шифрування в Python, уразливість.

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

***Тема 15.** Асиметричні шифри та системи. Математичні та алгоритмічні основи:*

Криптографія по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.

Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор – акселератор RSA;

Технології асиметричного шифрування в Python, уразливість.

***Тема 16.** Асиметричні шифри та системи. Технології реалізації та уразливість:*

Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.

Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда.

Технології асиметричного шифрування в Python, уразливість.

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

***Тема 17.** Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах:*

методи аутентифікація та ідентифікація суб'єктів на основі симетричних систем шифрування. Поняття майстер ключа та змінного ключа;

технології аутентифікація та ідентифікація в Python.

***Тема 18.** Електронний цифровий підпис, методи та засоби:*

встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та цифрового підпису;

аутентифікація та ідентифікація суб'єктів в протоколах відкритих замовлень. Поняття електронних чеку та квитанції;

багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

Цикл лабораторних робіт з дисципліни «Захист інформації в комп'ютерних системах» спрямовано на набуття практичних навичок реалізації та дослідження особливостей і

ефективності складових комплексної системи захисту корпоративної інформації як у вигляді окремих елементів, так і в синергетичному поєднанні в єдину систему.

Цикл лабораторних робіт побудовано на принципах нарощування функціональності комплексної системи захисту корпоративної інформації. Це реалізується в декількох аспектах:

евристичний синтез комплексної системи захисту корпоративної інформації;

дослідження особливостей комп'ютерних вірусів та створення системи протидії;

дослідження особливостей кібернетичного впливу на комп'ютерні системи та створення системи протидії;

розробка криптографічних систем захисту інформації та дослідження їх уразливості.

Питання вірусології та кібернетичної безпеки відпрацьовуються на реальному шкідливому програмному забезпеченні з використанням технологій віртуальних обчислювальних систем.

Питання розробки криптографічних систем захисту інформації та дослідження їх уразливості реалізується з використанням можливостей мови програмування високого рівня – Python.

Тематика лабораторних робіт:

***Лабораторна робота №1.** (2 год.) Дослідження процесів створення комплексної системи захисту корпоративної інформації:*

Розробка проекту КСЗІ для конкретного об'єкту інформаційної діяльності – комп'ютерної системи (встановлення категорії інформації, що захищається; дослідження каналів витоку, модель загроз; модель порушника; комплекс організаційних та технічних заходів і засобів захисту інформації; структура КСЗІ; дослідження ефективності КСЗІ).

***Лабораторна робота №2.** (2 год.) Дослідження процесів захисту інформації від комп'ютерних вірусів:*

Створення ізольованого віртуального середовища досліджень; генерація вірусів та дослідження їх сигнатур; дослідження ефективності детектування сигнатур вірусів різними програмними засобами; створення системи захисту інформації від комп'ютерних вірусів та дослідження її ефективності.

***Лабораторна робота №3.** (2 год.) Дослідження процесів захисту інформації від кібернетичних атак:*

Створення ізольованого віртуального середовища досліджень; дослідження уразливості оточення до кібернетичних впливів; створення системи захисту інформації від кібернетичних впливів та дослідження її ефективності.

***Лабораторна робота №4.** (2 год.) Дослідження технологій традиційного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології традиційного шифрування за заданим алгоритмом та дослідження їх уразливості.

***Лабораторна робота №5.** (2 год.) Дослідження технологій блочного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології блочного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №6. *(2 год.) Дослідження технологій симетричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології симетричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №7. *(2 год.) Дослідження технологій асиметричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології асиметричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №8. *(2 год.) Дослідження технологій аутентифікації та ідентифікації в розподілених комп'ютерних системах:*

Розробка скрипта в Python, що реалізує технології електронного цифрового підпису та дослідження ефективності процесів аутентифікації та ідентифікації в розподілених комп'ютерних системах.

6. Самостійна робота студента/аспіранта

В якості самостійної роботи студента застосовується підготовка до аудиторних занять, проведення розрахунків за первинними даними, отриманими на лабораторних заняттях, розв'язок задач, виконання модульної контрольної роботи. Загальний обсяг часу, що відводиться на самостійну роботу складає – 66 годин.

● Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

В процесі вивчення навчальної дисципліни вітається та заохочується:

- *колегіальність взаємовідносин в процесі реалізації освітнього процесу;*
- *своєчасність надання звітності за усіма формами контролю;*
- *дотримання норм академічної доброчесності.*

Порядок оформлення та надання звітності за усіма формами та порядок оцінювання результатів регламентується порядком, вказаному у завданнях: на лабораторні роботи; модульної контрольної роботи; методичних матеріалів із проведення заліку.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

РСО з дисципліни, семестровий контроль з якої передбачений у вигляді екзамену, розробляється за типом РСО-2 і складається з двох складових:

- *стартової – призначена для оцінювання заходів поточного контролю впродовж семестру (**Rc**)*
- *екзаменаційної – призначена для оцінювання окремих запитань (завдань) на екзамені. (**Re**)*

Рекомендований розмір стартової складової РСО дорівнює 60 балів, екзаменаційної складової – 40 балів.

Стартові бали формуються як сума рейтингових балів, отриманих здобувачем за результатами заходів поточного контролю, заохочувальних та штрафних балів.

Після оцінювання відповідей здобувача на екзамені (або виконання екзаменаційної контрольної роботи) викладач підсумовує стартові бали та бали за екзамен, зводить до рейтингової оцінки та переводить до оцінок за університетською шкало.

R = Rc + Re

Види контролю з навчальної дисципліни:

1. Виконання та захист 8-ми лабораторних робіт.

2. Виконання тестової роботи

3. Екзамен.

Таблиця 1

Оцінювання окремих видів навчальної роботи студента (у балах)

Вид навчальної роботи	**Всього за видом роботи**
Виконання та захист лабораторної роботи № 1	6
Виконання та захист лабораторної роботи № 2	6
Виконання та захист лабораторної роботи № 3	6
Виконання та захист лабораторної роботи № 4	6
…	
Виконання та захист лабораторної роботи № 8	8
Виконання лабораторних робіт **Rл**	50
Тест **Rk**	10
Усього за семестр **Rc= Rл + Rк**	**60**
Екзамен **Re**	**40**
Усього за семестр: (**R = Rc + Re**)	**100**

Система рейтингових (вагових) балів та критерії оцінювання

Звітність	*Лр 1*	*Лр 2*	*Лр 3*	*Лр 4*	*Лр 5*	*Лр 6*	*Лр 7*	*Лр 8*	*МК*	*СУМА*	*Екзамен*	*Сумма*
Високий рівень	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*8*	*10*	*60*	*40*	*100*

1. Виконання та захист 8 лабораторних робіт

*Ваговий бал за одну роботу максимум – 6-8. Максимальна кількість балів за всі лабораторні роботи дорівнює 6 * 7 + 8 = 50 балів.*

1.1. Охайне оформлення протоколу лабораторної роботи – 2 бал.

1.2. Своєчасний захист роботи – 1 бал.

1.3. Виконання роботи в повному обсязі (теоретичне обґрунтування, практичний результат, аналіз та висновки) – 6-8 бали.

2.Тест

Максимальна кількість балів за тест - 10 балів.

3. Екзамен

Максимальна кількість - 40 балів.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	*Відмінно*
94-85	*Дуже добре*
84-75	*Добре*
74-65	*Задовільно*

64-60	*Достатньо*
Менше 60	*Незадовільно*
Не виконані умови допуску	*Не допущено*

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль

Перелік теоретичних питань.

1. Розкрити сутність понять: захист інформації; комплексна система захисту інформації; загрози інформації.

2. Що таке інформаційна безпека, що вона в себе включає?

3. Розкрити сутність та складові технічного захисту інформації.

4. Охарактеризуйте національне законодавство у сфері захисту інформації.

5. Дайте характеристику стандартам інших держав у сфері захисту інформації.

6. Властивості інформації.

7. Категорії інформації.

8. Загрози інформації.

9. Модель порушника.

10. Модель загроз.

11. Політика безпеки.

12. Комплексна система захисту інформації.

13. Класифікація вірусів.

14. Алгоритм роботи файлових вірусів.

15. Розкрити сутність роботи макровірусів.

16. Методи виявлення вірусів.

17. Типи антивірусних програм.

18. Критерії ефективності антивірусних програм.

19. Склад системи забезпечення захисту від комп'ютерних вірусів.

20. Класифікація і характеристика програмних засобів віддаленого управління.

21. Що таке комп'ютерна атака та її етапи.

22. Типи та сценарії комп'ютерних атак.

23. Розкрити зміст підготовчого етапу здійснення комп'ютерної атаки.

24. Розкрити зміст підготовчого етапу реалізації комп'ютерної атаки.

25. Розкрити зміст підготовчого завершального етапу комп'ютерної атаки.

26. Класифікація програмних засобів захисту від комп'ютерних атак.

27. Захист від комп'ютерних атак з використанням брандмауерів.

28. Сканер безпеки. Сутність, призначення, функціонування.

29. Комплексна система захисту інформації від комп'ютерних атак.

30. Технологія віртуальних приватних мереж як засіб захисту від комп'ютерних атак.

31. Критерії ефективності антивірусних програм.

32. Технології захисту інформації з використанням криптоалгоритмів.

33. Конвеєр задач криптографічного захисту та їхня сутність.

34. Класифікація шифроалгоритмів.

35. Пояснити сутність понять: криптологія, кодування, шифрування інформації

36. Сутність, призначення типи класичних шифрів.

37. Показники ефективності криптоалгоритмів.

38. Сутність, алгоритм, переваги і недоліки шифру Цезаря.

39. Сутність, алгоритм, переваги і недоліки шифру скитала.

40. Сутність, алгоритм, переваги і недоліки шифру Віженера.

41. Сутність, алгоритм, переваги і недоліки шифру Уітстона.

42. Сутність, алгоритм, переваги і недоліки потокових шифрів

43 Сутність, алгоритм, переваги і недоліки шифрування методом гамування.

44. Криптографічний аналіз. Основні методи реалізації та їх сутність.

45. Алгоритми блочного шифрування – сутність, властивості, реалізація.

46. Характеристики стійкості алгоритмів блочного шифрування.

47. Алгоритми потокового шифрування: сутність, приклади, реалізація.

48. Сучасні криптоалгоритми симетричного шифрування.

49. Симетричні криптографічні системи та їх стандарти.

50. Асиметричні криптографічні системи та їх стандарти.

51. Технології аутонтифікації та ідентифікації в компютених системах.

52. Реалізація технологій аутентифікації та ідентифікації з використанням електронного цифрового підпису.

53. Шифр Вернама;

54. Шифрування методом гамування.

55. Шифри перестановки:

56. Шифри перестановки без використання ключів;

57. Шифри перестановки з використанням ключів.

58. Генератори випадкових послідовностей для криптографічних систем.

59. Стандарт симетричного блокового шифрування Data Encryption Standard (DES).

60. Багатокаскадний алгоритм DES.

61. Симетричний алгоритм блокового шифрування даних IDEA

62. Криптографічна система RSA.

Перелік практичних питань.

1. Розробити комплексну систему захисту інформації на об'єкт інформаційної діяльності – локальна обчислювальна мережа лабораторії з розробки прикладного програмного забезпечення в банківській сфері, що включає 5 посадових осіб.

2. Розробити модель порушника та модель загроз об'єкту інформаційної діяльності – локальна обчислювальна мережа лабораторії з розробки прикладного програмного забезпечення в сфері національної безпеки та оборони, що включає 8 посадових осіб.

3. Розробити технічне завдання на створення КСЗІ на об'єкті інформаційної діяльності – локальна обчислювальна мережа лабораторії з розробки прикладного програмного забезпечення в сфері автоматизації управління виробничими процесами, що включає 12 посадових осіб.

4. Розробити систему захисту інформації від її витоку технічними каналами на об'єкті інформаційної діяльності – локальна обчислювальна мережа лабораторії з розробки криптографічних систем захисту інформації, що включає 22 посадових особи.

5. Розробити систему протидії кібернетичним загрозам на об'єкті інформаційної діяльності – локальна обчислювальна мережа з доступу до глобальних мереж, що використовується в лабораторії з розробки програмного забезпечення за технологіями розподілених високошвидкісних обчислень. Лабораторія включає 15 посадових особи.

6. Розробити систему протидії кібернетичним загрозам на об'єкті інформаційної діяльності – локальна обчислювальна мережа з доступу до глобальних мереж, що використовується в лабораторії з розробки програмного забезпечення за технологіями розподілених високошвидкісних обчислень. Лабораторія включає 15 посадових особи.

6. Розробити проект документів для сертифікації лабораторії, що включає локальну обчислювальну мережу на якій реалізується розробка криптоалгоритмів. Лабораторія включає 5 посадових особи.

7. Розробити комплексну систему захисту інформації на об'єкті інформаційної діяльності – локальна обчислювальна мережа з доступу до глобальних мереж, що використовується в лабораторії з розробки програмного забезпечення за технологіями розподілених високошвидкісних обчислень. Лабораторія включає 12 посадових особи.

8. Розробити криптографічну систему та її програмну компоненту з використанням шифра Цезаря. Шифруванню підлягають файли англомовного тексту. Провести

криптографічний аналіз розробленої криптографічної системи.

9. Розробити криптографічну систему та її програмну компоненту з використанням шифра скитала. Шифруванню підлягають файли англомовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

10. Розробити криптографічну систему та її програмну компоненту з використанням шифра Віженера. Шифруванню підлягають файли англомовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

11. Розробити криптографічну систему та її програмну компоненту з використанням шифра Уітстона. Шифруванню підлягають файли англомовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

12. Розробити криптографічну систему та її програмну компоненту з використанням подвійного шифра Цезаря. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

13. Розробити криптографічну систему та її програмну компоненту з використанням подвійного шифра скитала. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

14. Розробити криптографічну систему та її програмну компоненту з використанням подвійного шифра Віженера. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

15. Розробити криптографічну систему та її програмну компоненту з використанням подвійного шифра Уітстона. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

16. Розробити криптографічну систему та її програмну компоненту з використанням афінного шифру. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

17. Розробити криптографічну систему та її програмну компоненту з використанням афінного шифру. Шифруванню підлягають файли англомовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

18. Розробити криптографічну систему та її програмну компоненту з використанням подвійного афінного шифру. Шифруванню підлягають файли україномовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

19. Розробити криптографічну систему та її програмну компоненту та її програмну компоненту з використанням подвійного афінного шифр. Шифруванню підлягають файли англомовного тексту. Провести криптографічний аналіз розробленої криптографічної системи.

20. Розробити криптографічну систему та її програмну компоненту з використанням потокового RC4 шифру. Шифруванню підлягають файли україномовного тексту.

21. Розробити криптографічну систему та її програмну компоненту з використанням потокового RC4 шифру. Шифруванню підлягають файли англомовного тексту.

22. Розробити криптографічну систему та її програмну компоненту з використанням стандарту симетричного шифрування Data Encryption Standard (DES). Шифруванню підлягають файли україномовного тексту..

23. Розробити криптографічну систему та її програмну компоненту з використанням стандарту симетричного шифрування Data Encryption Standard (DES). Шифруванню підлягають файли англомовного тексту.

24. Розробити криптографічну систему та її програмну компоненту з використанням подвійного алгоритму DES. Шифруванню підлягають файли україномовного тексту.

25. Розробити криптографічну систему та її програмну компоненту з використанням подвійного алгоритму DES. Шифруванню підлягають файли англомовного тексту.

26. Розробити криптографічну систему та її програмну компоненту з використанням потрійного алгоритму DES. Шифруванню підлягають файли україномовного тексту.

27. Розробити криптографічну систему та її програмну компоненту з використанням

потрійного алгоритму DES. Шифруванню підлягають файли англомовного тексту.

28. Розробити криптографічну систему та її програмну компоненту з використанням алгоритму цифрового підпису DSA. Шифруванню підлягають файли україномовного тексту.

29. Розробити криптографічну систему та її програмну компоненту з використанням алгоритму цифрового підпису DSA. Шифруванню підлягають файли англомовного тексту.

30. Розробити криптографічну систему та її програмну компоненту з використанням алгоритму цифрового підпису ECDSA. Шифруванню підлягають файли україномовного тексту.

31. Розробити криптографічну систему та її програмну компоненту компоненту з використанням алгоритму цифрового підпису ECDSA. Шифруванню підлягають файли англомовного тексту.

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри обчислювальної техніки, доктором технічних наук, професором Писарчуком Олексієм Олександровичем.

Ухвалено кафедрою обчислювальної техніки (протокол № 10 від 25.05.2022).

Погоджено Методичною комісією факультету інформатики та обчислювальної техніки (протокол № 10 від 09.06.2022).

…