МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ
Кафедра автоматизації виробничих процесів

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва курсу	ЗАХИСТ ІНФОРМАЦІЇ ТА КОМП`ЮТЕРНА КРИПТОГРАФІЯ
Викладач (-і)	Олександр ДІДИК, кандидат технічних наук, доцент, завідувач кафедри автоматизації виробничих процесів
Контактний тел.	+38(050) 487-12-64
E-mail:	Didyk_s79@ukr.net
Обсяг та ознаки дисципліни	Вибіркова дисципліна, змістових модулів – 2. Форма контролю: залік. Загальна кількість кредитів – 4, годин – 120, у т.ч. лекції – 28 годин, практичні заняття – 14 годин, самостійна робота – 78 годин. Формат: очний (offline / face to face) / дистанційний (online). Мова викладання: українська. Рік викладання – 2023.
Консультації	Консультації проводяться відповідно до Графіку, розміщеному в інформаційному ресурсі moodle.kntu.kr.ua; у режимі відеоконференцій Zoom, через електронну пошту, Viber, Messenger, Telegram за домовленістю.
Пререквізити	Після вивчення дисциплін «Теорія інформації», «Основи збору, передачі та обробки інформації», «Комп’ютерні мережі»

1. Мета і завдання дисципліни

Забезпечення безпечної діяльності комп'ютерних систем необхідне для будь-яких підприємств і установ починаючи від державних організацій і закінчуючи невеликими приватними фірмами, не залежно від виду їх діяльності. Розходження полягає лише в засобах, методах та в обсязі забезпечення безпеки.

Якщо пріоритет збереження безпеки особистості є природним, то пріоритет інформації над матеріальними цінностями вимагає більш докладного розгляду. Це стосується не тільки інформації, що складає державну чи комерційну таємницю, але і відкритої інформації.

Мета вивчення дисципліни є надання студентам знань про загальні відомості щодо захисту інформації, потенційних загроз та проблем захисту даних в локальних системах та комп'ютерних мережах.

Завдання вивчення дисципліни передбачає вивчення методів і засобів захисту інформації в комп'ютерних системах, основних засад інформаційної безпеки, класифікацію та принципи побудови систем захисту.

Студенти при вивченні дисципліни отримують знання про загальні відомості щодо захисту інформації, класифікацію загроз інформації та міри протидії ним, класифікацію та особливості комп'ютерних вірусів, основи захисту інформації в комп'ютерних мережах.

2. Результати навчання

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати:

- класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів,
- захищати інформацію персонального комп'ютера,
- управляти доступом та адмініструванням мереж,
- використовувати системи кодування інформації та її стискування,
- розробляти індивідуальні системи управління доступом і захистом інформації.

вміти:

- використовувати комп’ютерні криптографічні,
- стеганографічні системи,
- антивірусні засоби.

3. Політика курсу та академічна доброчесність

Очікується, що здобувачі вищої освіти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті здобувачі вищої освіти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення вибіркових навчальних дисциплін та формування індивідуального навчального плану ЗВО; Кодексу академічної доброчесності ЦНТУ.

4. Програма навчальної дисципліни

Змістовий модуль 1.

Тема 1. Поняття інформаційної безпеки та захисту інформації. Основні складові інформаційної безпеки.

Основні складові інформаційної безпеки. Важливість і складність

проблеми інформаційної безпеки. Загрози. Основні визначення і критерії класифікації погроз. Найбільш розповсюджені погрози приступності. Деякі приклади погроз приступності.

Тема 2. Законодавчий, адміністративний та процедурний рівні інформаційної безпеки.

Рівні забезпечення інформаційної безпеки. Законодавчий рівень інформаційної безпеки. Адміністративний рівень інформаційної безпеки. Процедурний рівень інформаційної безпеки. Програмно-технічний рівень інформаційної безпеки.

Тема 3. Програмно-технічний рівень інформаційної безпеки.

Ідентифікація і аутентификация, керування доступом. Парольна аутентификация. Одноразові паролі. Аутентифікація за допомогою сервера аутентифікації Kerberos. Ідентифікація/аутентифікація за допомогою біометричних даних. Керування доступом. Протоколювання й аудит. Шифрування. Контроль цілісності. Екранування.

Тема 4. Захист персональної ЕОМ.

Шкідливі зовнішні фізичні фактори. Шкідливе ПЗ. Помилки в ПЗ та "чорні ходи" в ньому (зокрема це стосується і операційних систем). Невірне адміністрування. Можливість фізичного доступу зловмисника до ЕОМ.

Змістовий модуль 2.

Тема 5. Атаки на мережеві системи.

Основні компоненти мереж, що атакуються: Сервера, робочі станції, середовище передачі інформації, вузли комутації мереж

Тема 6. Криптографія. Основні поняття.

Основні поняття та визначення. Вимоги до криптографічних систем. Найпростіші симетричні криптосистеми.

Тема 7. Симетричні криптосистеми. Блочні шифри. Приклади блочних шифрів.

Генерація блочних шифрів. Режими застосування блочних шифрів. Алгоритм блочного шифрування DES. Алгоритм RC6.

Тема 8. Асиметричні криптосистеми.

Асиметрична криптосистема Ель-Гамаля. Криптосистема Рівеста-Шаміра-Ейделмана (RSA). Електронні цифрові підписи. Стандарт цифрового підпису DSS. Функції хешування

5. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю здобувачів, усне опитування, письмовий контроль.

Рейтинг студента із засвоєння дисципліни визначається за 100 бальною системою, у тому числі: перший рубіжний контроль – 50 балів, другий рубіжний контроль – 50 балів.

Семестровий залік полягає в оцінці рівня засвоєння здобувачем вищої

освіти навчального матеріалу на лекційних, практичних заняттях і виконання індивідуальних завдань.

Поточне тестування та самостійна робота		Сума
Змістовий модуль 1	Змістовий модуль 2	100
Т1-Т6	Т7- Т12	
50	50	

6. Рекомендована література

1. Вербіцький О.В. Вступ до криптології. - Львів: Науково-технічна література, 1998.-248с.
2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2004. – 216 с.
3. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
4. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
5. Коваленко М.М. Комп’ютерні віруси і захист інформації. Навчальний посібник / М.М. Коваленко. – К.: Наукова думка, 1999. – 268 с.

Розглянуто і схвалено на засіданні кафедри АВП, Протокол №1 від «15» серпня 2022 р.