Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра
технічної кібернетики

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*126 Інформаційні системи та технології*
Освітня програма	*Інформаційне забезпечення робототехнічних систем*
Статус дисципліни	*нормативна*
Форма навчання	*очна(денна)/дистанційна/змішана*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*120 годин*
Семестровий контроль/ контрольні заходи	*екзамен*
Розклад занять	*Лекції:* *середа 1 пара (8.30-10.05)* *Практичні заняття:* *середа 2-4 пара (10.25-12.00, 12.20-13.55, 14.15-15.50)*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *д.т.н., доц., доц. кафедри ТК Корнага Я.І.,* slovyan_k@ukr.net Практичні заняття: *д.т.н., доц., доц. кафедри ТК Корнага Я.І.,* slovyan_k@ukr.net
Розміщення курсу	https://ecampus.kpi.ua

Програма навчальної дисципліни

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

Мета вивчення дисципліни – набуття ключових фахових компетентностей, теоретичних знань і практичних навичок з захисту інформації для подальшого застосування у різних сферах професійної діяльності.
Предметом вивчення дисципліни є технології, методи та засоби інтелектуального аналізу даних.
Завдання вивчення дисципліни: – оволодіння основними поняттями безпеки інформації.
Навчальна дисципліна покликана допомогти студенту отримати:
знання:

- основні тенденції розвитку безпеки інформації і моделі потенціальних загроз;
- термінологію і основні поняття теорії захисту інформації;
- нормативні документи та міжнародні стандарти захисту інформації;
- основні загрози безпеці інформації в інформаційно-комунікаційних системах;
- методи захисту інформації на рівні операційних систем;
- механізми і технології захисту в розподілених системах;
- порядок створення, введення у дію та супроводження захищених систем.

вміння:

- визначати джерела, ризики та форми атак на інформацію;
- розробляти політику безпеки організації відповідно до стандартів та нормативно-правових документів;
- розробляти комплексну систему захисту інформації організації;
- організовувати багаторівневу систему захисту інформації мережі.

досвід:

- проектування та розробка захищених систем;
- кваліфікованої експлуатації комп'ютерів, управління його режимами, проведенням модернізації комп'ютерної техніки для розроблення КСЗЗІ;
- аналізувати моделі комп'ютерів з точки зору використання в комп'ютеризованих та робототехнічних системах та впливу їх характеристик на основні показники системи управління в цілому.

Компетентності
Інтегральна компетентність Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі інформаційних систем, що характеризується комплексністю та невизначеністю умов із застосування теорій та методів інформаційних технологій.
Загальні компетентності
КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ 2. Здатність застосовувати знання у практичних ситуаціях.
КЗ 3. Здатність до розуміння предметної області та професійної діяльності
КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.
КЗ 6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
Спеціальні (фахові, предметні) компетентності
КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики захисту інформації та кібербезпеки під час виконання функціональних завдань та обов'язків
КС 7. Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення
КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).
Програмні результати навчання
ПР 2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій.

ПР 25. Виявляти вразливості і загрози інформації в інформаційних системах, обґрунтовано обирати механізми та технології захисту.

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

Пререквізити – Спеціальні розділи математики, Програмування, Операційні системи, Теорія алгоритмів, Теорія ймовірностей.
Постреквізити – Проектування інформаційних систем, Теорія мереж інтернет, WEB – технології, основи front-end технологій, основи back-end технологій.

3. Зміст навчальної дисципліни

Розділ 1. Загальні принципи інформаційної безпеки

1.1. Інформаційна безпека комп'ютеризованих систем управління
1.2. Теоретичні основи захисту інформації
1.3. Будова системи захисту інформації
1.4. Роль і розвиток стандартів інформаційної безпеки
1.5. Нормативно-правова база України із захисту інформації

Розділ 2. Криптографічні методи захисту інформації

2.1. Принципи криптографічного захисту інформації
2.2. Симетричні криптографічні системи
2.3. Асиметричні криптографічні системи
2.4. Хешувальні функції
2.5. Електронний цифровий підпис
2.6. Управління криптографічними ключами
2.7. Криптографічний аналіз
2.8. Криптографічні методи аутентифікації і перевірки цілісності

Розділ 3. Захист інформації в розподілених інформаційно-комунікаційних системах

3.1. Безпека мережних протоколів і прикладних служб Інтернету
3.2. Захист інформації на основі мережних екранів
3.3. Забезпечення захисту передачі даних на різних рівнях моделі OSI
3.4. Засоби захисту операційних систем Windows та UNIX
3.5. Захист інформації в системах управління базами даних
3.6. Захист інформації в електронних платіжних системах

Розділ 4. Розробка програмного забезпечення, стійкого до злому

4.1. Типові вразливості програмного забезпечення
4.2. Засоби захисту програмного забезпечення
4.3. Технології створення захищеного коду

Розділ 5. Створення та супроводження захищених систем

5.1. Створення комплексної системи захисту та кваліфікаційний аналіз засобів і систем захисту інформації
5.2. Супроводження комплексної системи захисту інформації

4. Навчальні матеріали та ресурси

Основна література

1. *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. — Київ, Видавнича група БХВ, 2009, – 608 с.
2. *Шаньгин В.Ф.* Защита компьютерной информации. М:, ДМК Пресс, 2008, – 544с.
3. *Ященко В.В.* Введение в криптографию. М:, МЦНМО, 2008, – 272с.

Додаткова література

4. *Кузнецов О.О., Євсеєв С.П., Король О.Г.* Захист інформації в інформаційних системах. Харків: Вид. ХНЕУ, 2011. – 510 с.
5. *Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки татехнічного захисту інформації., 2012. – 104 с.*

6. *В.В.Домарев.* Защита информации и безопасность комьютерних систем. 2009.
7. *Бриль В.М., Бриль Ю.В.* Захист інформації в сучасних та перспективних системах обробки даних.- К., 2008.
8. *Пономаренко В.С.* Информационные технологии и защита информации в информационно-коммуникационных системах. 2015. – 486 с.
9. *Кузнецов О.О., Євсеєв С.П., Король О.Г.* Захист інформації в інформаційних системах. методи традиційної криптографії. Харків: Вид. ХНЕУ, 2010.– 316 с.

Інформаційні ресурси

- https://ecampus.kpi.ua

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ лекції	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1.	**Загальні принципи інформаційної безпеки** *1. Інформаційна безпека комп'ютеризованих систем управління.* Основні поняття. Завдання захисту інформації. Загрози і вразливості. Об'єкти захисту та їх властивості. Причини порушення безпеки комп'ютерних систем. Модель загроз. Модель порушника. ([1] с.9, [2] с.35) *2. Теоретичні основи захисту інформації.* Основні поняття теорії захисту інформації. Математичні моделі безпеки. Моделі дискреційної політики безпеки. Моделі мандатної політики безпеки. ([1] с.14, [2] с.35) *3. Будова системи захисту інформації.* Рівні інформаційно-комунікаційної системи. Комплексна система захисту інформації. Підсистема керування доступом. Підсистема ідентифікації та автентифікації. Підсистема аудиту. Підсистема забезпечення цілісності. Криптографічна підсистема.
2.	*1. Роль і розвиток стандартів інформаційної безпеки.* Призначення стандартів інформаційної безпеки. «Критерії оцінювання захищеності комп'ютерних систем» Міністерства оборони США («Оранжева книга»). Класи безпеки комп'ютерних систем. Європейські критерії інформаційної безпеки. Функціональні критерії та критерії адекватності. Базові поняття критеріїв. Профіль та проект захисту продукту інформаційних технологій. ([1] с.20, [2] с.37) *2. Нормативно-правова база України із захисту інформації.* Законодавча і нормативна база захисту інформації в Україні. Оцінювання захищеності інформації, що обробляється в комп'ютерних системах. Керівні документи з вимогами до захисту інформації в комп'ютерних системах різних типів. ([1] с.22, [2] с.37)
3.	**Технології захисту інформації** *1. Принципи криптографічного захисту інформації.* Основні поняття криптографічного захисту інформації. Крипостійкість та криптоаналіз алгоритмів шифрування. Поняття криптографічної системи. Застосування криптографічних алгоритмів. Класичні методи шифрування даних. Шифри перестановки та заміни. Метод гамування. Блочні і поточні шифри. ([1] с.47, [2] с.198)
4.	*1. Симетричні криптографічні системи.* Концепція криптографічних систем з секретним ключем. Модель симетричної криптосистеми. Стандарти шифрування IDEA, DES та AES. Основні режими роботи симетричних алгоритмів шифрування. Комбінування блочних алгоритмів. Особливості використання симетричних алгоритмів шифрування. ([1] с.93, [7] с.96)
5.	*1. Асиметричні криптографічні системи.* Концепція криптографічних систем з відкритим ключем. Однонаправлені функції. Тести простоти. Криптосистема шифрування даних RSA. Безпека та швидкодія системи RSA. Схеми шифрування Поліга-Хелмана та Ель Гамаля. Криптосистеми на основі еліптичних кривих. Комбінований метод шифрування. ([1] с.102, [2] с.235, [4] с.35)

6.	*1. Хешувальні функції.* Властивості і застосування хеш-функцій. Функції хешування MD. Функції хешування SHA. Колізії хеш-функцій. Криптографічний аналіз хеш-функцій. ([1] с.115, [2] с.240)
7.	*1. Електронний цифровий підпис.* Функції цифрового підпису. Формування підпису. Алгоритми цифрового підпису RSA, Ель-Гамаля, DSA. Сліпі підписи. Незаперечні підписи. Стійкість ЕЦП. Криптоаналіз ЕЦП. ([1] с.155, [2] с.257, [4] с.58).
8.	*1. Управління криптографічними ключами.* Практика адміністрування ключами. Генерування ключів. Генерування псевдовипадкових послідовностей. Генератори. Розрядність ключів. Збереження ключів. Розподіл ключів. Метод Діффі-Хелмана. Прямий обмін ключами між користувачами. Протокол ECKEP. ([1] с.147)
9.	*1. Криптографічний аналіз.* Функції криптоаналізу. Різницевий криптоаналіз. Лінійний криптоаналіз. Криптоаналіз алгоритмів шифрування. Криптоаналіз хеш-функцій. Надійність криптосистем. ([1] с.201, [2] с.15, [4] с.151)
10.	*1. Методи аутентифікації і перевірки цілостності.* Ідентифікація та перевірка істинності користуваяа. Взаємна перевірка істинності користувачів. Біометрична ідентификація користувачів. Сувора ідентифікація на основі симетричних та асиметричних алгоритмів. Протоколи ідентифікації з нульовою передачею знань. Паралельна схема ідентифікації з нульовою передачею знань. Схема ідентифікації Гіллоу-Кіускуотера. ([1] с.220, [2] с.32)
11.	**Захист інформації в розподілених інформаційно комунікаційних системах** *1. Безпека мережних протоколів і прикладних служб Інтернету.* Безпека протоколів прикладного рівня. Транспортні протоколи. Стек протоколів IP. Безпека прикладних служб Інтернету. Системи виявлення атак. ([1] с.223, [2] с.25)
12.	*1. Захист інформації на основі мережних екранів.* Особливості функціонування міжмережних екранів. Основні компоненти міжмережних екранів. Основні схеми захисту мереж на основі міжмережних екранів. ([1] с.239, [2] с.88)
13.	*1. Забезпечення захисту передачі даних на різних рівнях моделі OSI.* Віртуальні захищені мережі. Можливості і проблеми створення захищеної віртуальної мережі на канальному, мережевому та сеансовому рівнях моделі OSI. Захист передачі даних на основі протоколу IPSec. Протоколи HTTPS, L2TP, SOCKS, SSL/TLS, SSH, SKIP. ([1] с.246, [2] с.108, [4] с.250)
14.	1. *Засоби захисту операційних систем Windows та UNIX.* Списки контролю доступу. Аутентифікація та управління доступом в системі Windows. Аутентифікація та управління доступом в системі UNIX. Принципи організації аудиту в операційних системах. Системний журнал в операційній системі UNIX. Журнал подій в операційній системі Windows. Шифруючі файлові системи в Windows та UNIX. Типи атак та засоби боротьби з ними в операційних системах. ([1] с.269, [2] с.150, [4] с.249)
15.	*1. Захист інформації в системах управління базами даних.* Основні вразливості СУБД. Системи розмеження доступу. Засоби підтримки цілістності інформації в СУБД. Реєстрація дій користувачів. Засоби підтримки високої готовності. ([1] с.286) *2. Захист інформації в електронних платіжних системах.* Принципи функціонування електронних платіжних систем. Електронні пластикові картки. Персональний ідентифікаційний номер. Безпека систем POS та банкоматів. Безпека електронних платежів у мережі Інтернет. Протоколи SET та SSL. ([1] с.322)
16.	**Розробка програмного забезпечення стійкого до взлому** *1. Типові вразливості програмного забезпечення.* Класифікація вад захисту. Класифікація помилок, що виникають у процесі розробки програмного забезпечення. Моделювання загроз. Шкідливе програмне забезпечення. Програмні закладки. Комп'ютерні віруси. Спеціальні хакерські утиліти. Принципи роботи та основні типи антивірусних програм. ([1] с.280, [2] с.156, [4] с.252) *2. Засоби захисту програмного забезпечення.* Загальні принципи забезпечення безпеки. Аналіз

	захищеності коду. Тестування захисту. Забезпечення конфіденційності. Засоби захисту програмного забезпечення від несанкціонованого завантаження. Захист інформації на машинних носіях. Захист залишків інформації. ([1] с.290, [2] с.146, [4] с.212)
17.	*1. Створення захищеного коду.* Вибір механізму керування доступом. Захист конфіденційних даних. Принцип мінімальних привілегій. Контроль вхідних даних. Запобігання помилок приведення до канонічного вигляду. Захист RPC, ActiveX-елементів та обєктів DCOM. Протидія атакам відмова в обслуговуванні. ([1] с.385)
18.	**Створення та супроводження захищених систем** *1. Створення комплексної системи захисту та кваліфікаційний аналіз засобів і систем захисту інформації.* Порядок проведення робіт зі створення комплексної системи захисту. Вимоги до комплексної системи захисту та політики безпеки. Розроблення технічного завдання до створення комплексної системи захисту інформації. Створення і впровадження комплексної системи захисту. Вимоги до кваліфікаційного аналізу. Організація державної експертизи. Сертифікація засобів технічного захисту інформації. ([1] с.385) *2. Супроводження комплексної системи захисту.* Завдання, функції, права і обов'язки служби захисту інформації. Організація заходів служби захисту інформації. Структура та зміст плану захисту інформації. ISO/IEC 27002 «Інформаційні технології — Методики безпеки — Практичні правила управління безпекою інформації». ([1] с.459, [2] с.314)

Практичні заняття (Комп'ютерний практикум)

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу та завдання на СРС)
1	**Розділ 1. Загальні принципи інформаційної безпеки** Встановлення та налаштування антивірусних програм. ([1] с.13, 21, [2] с.45, [9] с.4)
2	**Розділ 2. Технології захисту даних** Підсистема ідентифікації й автентифікації. ([1] с.36, [2] с.204, [9] с.8)
3	Підсистема реєстрації. ([1] с.46, [2] с.210, [9] с.15)
4	Підсистема розділення ролей. ([1] с.60, [9] с.12)
5	Симетричні алгоритми шифрування ([1] с.168, [9] с.12)
6	Асиметричні алгоритми шифрування ([1] с.180, [9] с.19)
7	Хешувальні функції ([1] с.198, [9] с.22)
8	Електронно цифровий підпис ([1] с.200, [9] с.12)
9	**Розділ 3. Захист інформації в розподілених інформаційно-комунікаційних системах** Перехоплення мережевого обміну. ([1] с.79, [7] с.103)
10	Міжмережеві екрани. ([1] с.110, 114, 119, [2] с.272)
11	Сканування TCP/IP мереж. ([1] с.129, 137, [2] с.272, [9] с.30)
12	Засоби аналізу захищеності. ([1] с.176, [2] с.273, [9] с.34)
13	Механізми захисту операційної системи Unix. ([1] с.176, [2] с.273, [9] с.34)
14	Механізми захисту операційної системи Windows. ([1] с.144)
15	Захист реєстру операційної системи Windows. ([1] с.200, [2] с.40)
16	Підсистема керування доступом. ([1] с.211, 216, , [2] с.30, [9] с.36)
17	**Розділ 4. Розробка програмного забезпечення стійкого до взлому** Створення API стійкого до взлому. ([1] с.303, [2] с.146, [9] с.22) Течії у мережах. ([1] с.337)
18	**Розділ 5. Створення та супроводження захищених систем** Розробка КСЗЗІ 1 рівня. ([1] с.391, [2] с.285)

Календарне планування лекційних та практичних занять

Номер лекції	Номер практичного заняття	Дата проведення
Лекція 1	Заняття 1	03.02.2021
Лекція 2	Заняття 2	10.02.2021
Лекція 3	Заняття 3	17.02.2021
Лекція 4	Заняття 4	24.02.2021
Лекція 5	Заняття 5	03.03.2021
Лекція 6	Заняття 6	10.03.2021
Лекція 7	Заняття 7	17.03.2021
Лекція 8	Заняття 8	24.03.2021
Лекція 9	Заняття 9	31.03.2021
Лекція 10	Заняття 10	07.04.2021
Лекція 11	Заняття 11	14.04.2021
Лекція 12	Заняття 12	21.04.2021
Лекція 13	Заняття 13	28.04.2021
Лекція 14	Заняття 14	05.05.2021
Лекція 15	Заняття 15	12.05.2021
Лекція 16	Заняття 16	19.05.2021
Лекція 17	Заняття 17	26.05.2021
Лекція 18	Заняття 18	02.06.2021

6. Самостійна робота студента/аспіранта

Самостійна робота студентів складається з:

- підготовки до аудиторних занять (лекцій та комп'ютерних практикумів),
- виконання контрольної роботи (https://classroom.google.com),

Самостійна робота

№ з/п	Назва розділу, теми (окремого питання), що виноситься на самостійне опрацювання	Кількість годин СРС
1.	Вивчення етапів розвитку стандартів у галузі захисту інформації в комп'ютерних системах. . ([1] с.9, [2] с.35)	4
2.	Вивчення основних стандартів створення електронного цифрового підпису. ([1] с.47, [2] с.198) Вивчення основних методів управління криптографічними ключами. ([1] с.54, [2] с.210) Вивчення основних методів криптоаналізу ([1] с.93, [7] с.96)	4
3.	Вивчення основних методів захисту корпоративних мереж з використанням міжмережних екранів. ([1] с.80**,** [4] с.189, [7] с.76) вивчення принципів функціонування основних захищених мережних протоколів на різних рівнях моделі OSI. ([1] с.85**,** [4] с.201, [7] с.77) вивчення основних принципів функціонування системи безпеки СУБД. ([1] с.93, [7] с.96)	6
4.	Вивчення основних вад і вразливостей програмного забезпечення та принципів роботи антивірусних програм. ([1] с.165, [2] с.257) Вивчення основних методів захисту програмного забезпечення та створення захищеного коду. ([1] с.147)	6
5.	Вивчення основних положень створення і супроводження комплексної системи захисту інформації. ([1] с.201, [2] с.15**,** [4] с.151)	10

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Форми організації освітнього процесу, види навчальних занять і оцінювання результатів навчання регламентуються Положенням про організацію освітнього процесу в Національному технічному університеті України «Київському політехнічному інституті імені Ігоря Сікорського».

Політика виставлення оцінок: кожна оцінка виставляється відповідно до розроблених викладачем та заздалегідь оголошених студентам критеріїв, а також мотивується в індивідуальному порядку на вимогу студента; у випадку не виконання студентом усіх передбачених навчальним планом видів занять (лабораторних робіт, тесту) до екзамену він не допускається; пропущені заняття обов'язково мають бути відпрацьовані.

Відвідування є обов'язковим (за винятком випадків, коли існує поважна причина, наприклад, хвороба чи дозвіл працівників деканату). Якщо студент не може бути присутніми на заняттях, він все одно несете відповідальність за виконання завдань, що проводились в комп'ютерному класі.

Порядок зарахування пропущених занять. Відпрацювання пропущеного заняття з лекційного курсу здійснюється шляхом підготовки і захисту реферату за відповідною темою у вигляді презентації. Захист реферату відбувається відповідно до графіку консультацій викладача, з яким можна ознайомитись на кафедрі. Відпрацювання пропущеного лабораторного заняття здійснюється шляхом самостійного виконання завдання і його захисту відповідно до графіку консультацій викладача.

Реферати також можуть підготувати студенти, у яких недостатньо рейтингових балів.

Політика академічної поведінки та доброчесності: конфліктні ситуації мають відкрито обговорюватись в академічних групах з викладачем, необхідно бути взаємно толерантним, поважати думку іншого. Плагіат та інші форми нечесної роботи неприпустимі. Всі індивідуальні завдання та курсову роботу студент має виконати самостійно із використанням рекомендованої літератури й отриманих знань та навичок. Цитування в письмових роботах допускається тільки із відповідним посиланням на авторський текст. Недопустимі підказки і списування у ході захисту лабораторних робіт, на контрольних роботах, на іспиті.

Норми академічної етики: дисциплінованість; дотримання субординації; чесність; відповідальність; робота в аудиторії з відключеними мобільними телефонами. Повага один до одного дає можливість ефективніше досягати поставлених командних результатів. При виконанні лабораторних робіт студент може користуватися ноутбуками. Проте під час лекційних занять та обговорення завдань лабораторних робіт не слід використовувати ноутбуки, смартфони, планшети чи комп'ютери. Це відволікає викладача і студентів групи та перешкоджає навчальному процесу. Якщо ви використовуєте свій ноутбук чи телефон для аудіо- чи відеозапису, необхідно заздалегідь отримати дозвіл викладача.

Дотримання академічної доброчесності студентів й викладачів регламентується кодекс честі Національного технічного університету України «Київський політехнічний інститут», положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського

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

Розподіл балів, які отримують студенти на заняттях

Види контролю	*бали*
Комп'ютерний практикум (18 робіт)	3
Контрольна робота (1 робота)	6

R=(3*18+6)=60

*Календарний контрол*ь: провадиться один раз на семестр як моніторинг поточного стану виконання вимог силабусу.

За результатами навчальної роботи за перші 7 тижнів максимально можлива кількість балів – 21 балів. На першій атестації (8-й та 9-й тиждень) студент отримує "зараховано", якщо його поточний рейтинг не менше 18 балів.

За результатами 13 тижнів навчання максимально можлива кількість балів – 39 балів. На другій атестації (14-й тиждень) студент отримує "зараховано", якщо його поточний рейтинг не менше 33 балів.

Семестровий контроль: екзамен

Умови допуску до семестрового контролю: семестровий рейтинг більше 30 балів.

На екзамені студент може отримати максимум 40 балів.

- повна відповідь - 40;
- часткова відповідь - 1…39;
- незадовільна відповідь - 0.

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 (<30)	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Теми рефератів для отримання додаткових балів:

1. Історія розвитку засобів захисту інформації.
2. Сфери застосування комплексної системи захисту інформації.

Робочу програму навчальної дисципліни (силабус):

Складено доцент, д.т.н., доцент, Корнага Я.І.

Ухвалено кафедрою ТК (протокол №10 від 29.04.2020р

Погоджено Методичною комісією факультету (протокол №10 від 21.05.2020 р)