

# ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ



**ЗАТВЕРДЖУЮ**

Декан факультету ІТ

Олег САВЕНКО

Підпис Ім'я, ПРІЗВИЩЕ

» 08 2023 р.

## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### Побудова захищених комп'ютерних систем

**Галузь знань** 12 – Інформаційні технології  
**Спеціальність** 125 – Кібербезпека  
**Рівень вищої освіти** Перший бакалаврський  
**Освітньо-професійна програма** Кібербезпека  
**Обсяг дисципліни** 8 кредитів ЄКТС  
**Шифр дисципліни** ВД8769  
**Мова навчання** Українська  
**Статус дисципліни** Вибіркова  
**Факультет** Інформаційних технологій  
**Кафедра** Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин							Форма семестрового контролю		
			Кредити ЄКТС	Години	Аудиторні заняття					Самостійна робота, у т.ч. ІРС	Курсовий проєкт	Курсова робота	Залік	Іспит
					Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття					
Очна (денна)	-	-	8	240	90	36	54			150			+	

Робоча програма складена Віктор ЧЕШУН канд. техн. наук, доц. Віктор ЧЕШУН  
 Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки  
 Протокол від 31.08.2023 № 1 Зав. кафедри Юрій КЛЬОЦ  
 Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій  
 Голова вченої ради факультету Олег САВЕНКО  
 Підпис Ім'я, ПРІЗВИЩЕ

# ПОБУДОВА ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Тип дисципліни

Вибіркова

Освітній рівень

Перший (бакалаврський)

Мова викладання

Українська

Кількість кредитів ЄКТС

8

Форми здобуття освіти

Очна денна

**Результати навчання.** Студент, який успішно завершив вивчення дисципліни, повинен: *знати*: основні поняття теоретичної, прикладної та законодавчої метрології; методи і засоби забезпечення єдності вимірювань; призначення та основні характеристики вимірювальних пристроїв; організацію, структуру та основні положення національної і міжнародної систем стандартизації із стандартизацією в галузі інформаційної безпеки включно; принципи впровадження стандартів та державного нагляду за їх дотриманням; загальні принципи сертифікації продукції, послуг, персоналу, систем управління (в тому числі в галузі інформаційної і кібербезпеки); вимоги державних стандартів України щодо оформлення текстової, програмної і графічної документації; *уміти*: вибирати засоби вимірювань, відповідні певному виду вимірювань; застосовувати методи вимірювання та оцінювати точність (похибки) вимірювань; користуватися спеціальною, довідковою та методичною літературою; застосовувати набуті знання для впровадження стандартів, розробки нормативних документів і здійснення контролю за їх дотриманням; використовувати нормативно-технічні документи і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки; розробляти і оформлювати супровідну текстову, програмну, конструкторську документацію технічного об'єкта у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо); *бути здатним*: обрати засоби вимірювань заданих величин, метод вимірювань і певну методику оцінки похибки виконаних вимірювань; діяти на основі нормативної бази України та вимог відповідних стандартів, у тому числі міжнародних (в галузі інформаційної та/або кібербезпеки включно); обґрунтувати необхідність впровадження нових стандартів та нормативно-технічної документації, а також здійснювати контроль за дотриманням їхніх вимог; використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел (державних та міжнародних стандартів й інших нормативних документів тощо) для ефективного рішення спеціалізованих задач професійної діяльності; оформити технічну документацію в процесі навчання (звіти, кваліфікаційну роботу тощо) і професійної діяльності (інструкції, звіти, нормативні документи, політики безпеки тощо) у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо); застосувати знання дисципліни для засвоєння навчальних дисциплін професійної підготовки.

**Зміст навчальної дисципліни.** Вимірювання: методи, засоби, точність і похибки вимірювань. Нормативно-правова і організаційна база метрології, національні і міжнародні метрологічні організації. Стандартизація – основні поняття, задачі, методи, органи, національна і міжнародна стандартизація. Основи стандартизації інформаційної і кібербезпеки. Єдина система конструкторської документації (ЄСКД). Єдина система програмної документації (ЄСПД). Сертифікація – основні поняття, завдання, методи, органи. Сертифікація в інформаційній і кібербезпеці.

**Запланована аудиторна робота:** кількість аудиторних годин – не менше 1/3 від загальної кількості годин, які заплановані для вивчення дисципліни.

**Методи навчання:** словесні, наочні та інтерактивні (лекції); практичні (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

**Форми оцінювання результатів навчання:** захист лабораторних робіт, тестування.

**Форма семестрового контролю:** залік.

**Навчальні ресурси:**

1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
3. Грабар І. Г., Гришук Р. В., Молодешька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир: ЖНАЕУ, 2019. 280 с.
4. Інформаційна безпека: навч. посіб./Бобало Ю. Я. та ін.; за заг. ред. д-ра техн. наук, проф. Бобала Ю. Я. та д-ра техн. наук, доц. Горбатого І. В. Львів: В-во Львівської політехніки, 2019. 580 с.
5. Жаровський Р.О. Захист інформації у комп'ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
6. Модульне середовище для навчання MOODLE. Доступ до ресурсу: <https://msn.khmnu.edu.ua/>.
7. Електронна бібліотека університету. Доступ до ресурсу: <http://library.khmnu.edu.ua/>.

**Викладач:** кандидат технічних наук, доцент Чешун В.М.

## ВСТУП

Дисципліна «Побудова захищених комп'ютерних систем» – вибіркова складова професійної підготовки магістрів в галузі інформаційних технологій зі спеціальності „Кібербезпека”.

Дисципліна „Метрологія, вимірювання, стандартизація та сертифікація” є однією з дисциплін загальної підготовки бакалаврів зі спеціальності „Кібербезпека”.

**Мета дисципліни.** Формування у студентів системи знань про методи і засоби побудови захищених комп'ютерних систем з набуттям здатності застосовувати знання у практичних ситуаціях, виконувати пошук, оброблення та аналіз інформації і застосовувати нормативну документацію, державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

**Предмет дисципліни.** Методи і засоби вимірювання електричних і неелектричних величин; Державна метрологічна служба України і міжнародні метрологічні організації; системи стандартизації і сертифікації України, ЄС та світу.

**Завдання дисципліни.** Забезпечити набуття компетентностей та досягнення результатів навчання відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

### **компетентності:**

КЗ 01. Здатність застосовувати знання у практичних ситуаціях.

КФ 01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

### **результати навчання:**

РН 1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки.

РН 8. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

Після вивчення дисципліни „Побудова захищених комп'ютерних систем” студент має:

### **знати:**

- методи і засоби забезпечення єдності вимірювань;
- призначення та основні характеристики вимірювальних пристроїв;
- організацію, структуру та основні положення національної і міжнародної систем стандартизації із стандартизацією в галузі інформаційної безпеки включно;
- принципи впровадження стандартів та державного нагляду за їх дотриманням;
- загальні принципи сертифікації продукції, послуг, персоналу, систем управління (в тому числі в галузі інформаційної і кібербезпеки);
- вимоги державних стандартів України щодо оформлення текстової, програмної і графічної документації.

### **уміти:**

- застосовувати методи вимірювання та оцінювати точність (похибки) вимірювань;
- користуватися спеціальною, довідковою та методичною літературою;
- використовувати нормативно-технічні документи і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;
- розробляти і оформлювати супровідну текстову, програмну, конструкторську документацію технічного об'єкта у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо).

### **бути здатним:**

- обрати засоби вимірювань заданих величин, метод вимірювань і певну методику оцінки похибки виконаних вимірювань;
- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел (державних та міжнародних стандартів й інших нормативних документів тощо) для ефективного рішення спеціалізованих задач професійної діяльності;
- оформити технічну документацію в процесі навчання (звіти, реферати, курсові проекти та кваліфікаційну роботу тощо) і професійної діяльності (інструкції, звіти, нормативні документи, політики безпеки тощо) у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо).

## СТРУКТУРА ЗАЛКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	практичні заняття	лабораторні роботи	самостійну роботу
Тема 1. Метрологія і вимірювання	16	-	24	68
Тема 2. Стандартизація і сертифікація побудови захищених комп'ютерних систем	20	-	30	82
<b>Разом:</b>	<b>36</b>	<b>-</b>	<b>54</b>	<b>150</b>

\* При плануванні лекцій за чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

# ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
<b>Тема 1. Метрологія і вимірювання</b>		
1	<b>Введення в дисципліну</b> Взаємозв'язок метрологія-стандартизація-сертифікація. Метрологія: основні поняття та визначення. Види фізичних величин. Міжнародна система одиниць. Основні одиниці системи СІ. Похідні та позасистемні одиниці системи СІ. Кратні та частинні одиниці системи СІ. Літ.: [2] с.25-52; [3] с.6-55; [4] с.120-123; [7] с.8-22; [8] с.7-46	4
2	<b>Вимірювальні засоби і прилади як інструмент метрології</b> Призначення і загальна класифікація вимірювальних засобів. Класифікація електронних вимірювальних приладів. Групи, підгрупи і шифри типів електронних вимірювальних приладів. Характеристики вимірювальних приладів. Вимоги до сучасних вимірювальних приладів. Літ.: [3] с.110-122; [4] с.127-130; [6] с.28-30, 53-90; [7] с.32-42, 53-100, 125-157; [8] с.47-88, 186-252	4
3	<b>Методи, точність і похибки вимірювань</b> Вимірювання як метрологічний процес. Стандартизовані визначення характеристик вимірювань. Методи вимірювань. Фактори, що впливають на точність вимірювань. Похибки – поняття та класифікація. Літ.: [1] стаття закону № 7; [2] с.55-66; [3] с.55-110; [4] с.123-127, 130-136; [6] с.13-27, 33-49; [8] с.89-119	4
4	<b>Нормативно-правова і організаційна база метрології</b> Нормативно-правова база метрології. Державна метрологічна система України. Міжнародні метрологічні організації. Система забезпечення єдності вимірювань. Літ.: [2] с.66-87; [3] с.155-200; [4] с.138-155; [7] с.23-31	4
<b>Тема 2. Стандартизація і сертифікація побудови захищених комп'ютерних систем</b>		
5	<b>Стандартизація – основні поняття, задачі, методи, органи</b> Поняття, задачі, рівні стандартизації Нормативні документи державної стандартизації Органи державної стандартизації України Органи міжнародної стандартизації Система стандартизації країн ЄС. Літ.: [2] с.88-147; [3] с.200-224; [4] с.7-51	4
6	<b>Єдина система конструкторської документації (ЄСКД) – введення. Оформлення текстової документації за ЄСКД.</b> Єдина система конструкторської документації (ЄСКД) - основні поняття, визначення та призначення (ДСТУ ГОСТ 2.001:2006). Сфера поширення стандартів ЄСКД. Склад, класифікація й позначення стандартів ЄСКД. Види конструкторських документів (ДСТУ 3321:2003). Комплектність конструкторських документів. Загальні правила оформлення графічних і текстових документів. Основні надписи конструкторських документів. Етапи розробки конструкторської документації. Загальні вимоги до текстових документів (ГОСТ 2.105-95). Оформлення пояснювальної записки. Порядок викладення тексту документів. Правила написання позначень і найменувань одиниць фізичних величин. Оформлення ілюстрацій і додатків. Побудова таблиць. Оформлення списку літератури. Оформлення специфікації. Літ.: [14] ; [17] с.101-106; [20] ; [21]	4

7	<p><b>Єдина система програмної документації (ЄСПД). Оформлення графічної документації і схем за ЄСКД та ЄСПД.</b>  Єдина система програмної документації. Види графічних документів за ЄСКД. Правила нанесення розмірів. Загальні вимоги до робочих креслень. Креслення деталі. Креслення складальні. Креслення загального виду. Різновиди схем і загальні вимоги до їх виконання. Схеми електричні структурні. Схеми електричні функціональні. Схеми електричні принципів. Схеми з'єднань.  Літ.: [14] ; [17] с.101-106; [20] ; [21] ; [22]</p>	4
8	<p><b>Стандартизація в галузі інформаційної і кібербезпеки</b>  Початок стандартизації в інформаційній безпеці. Критерії безпеки комп'ютерних систем міністерства оборони США TCSEC. Розвиток стандартів інформаційної і кібербезпеки Міжнародні стандарти для системи управління інформаційною безпекою ISO 270xx.  Літ.: [11] с.28-50; [12] с.81-92; [13] с.148-170 ; [28] с.91-108</p>	4
9	<p><b>Сертифікація – основні поняття, завдання, методи, органи. Сертифікація в інформаційній і кібербезпеці</b>  Сертифікація – основні поняття і визначення. Види сертифікації. Загальні принципи сертифікації. Система сертифікації. Норми і правила сертифікації. Акредитація органів сертифікації. Сертифікація систем управління інформаційною безпекою. Міжнародна сертифікація фахівців в галузі інформаційної і кібербезпеки.  Літ.: [2] с.233-302; [3] с.224-262; [4] с.51-116 ; [9] с.110-149</p>	4
<b>Разом:</b>		<b>36</b>

### Зміст лабораторних робіт

№ з/п	Тема лабораторного заняття	Кількість годин
1	Елементарні вимірювання неелектричних величин. Точність і похибки вимірювань. Літ.: [2] с.55-66; [3] с.55-110; [4] с.123-127, 130-136; [6] с.13-27, 33-49; [8] с.89-119	6
2	Ознайомлення з вимірювальним обладнанням лабораторії Літ.: [2] с.23-60; [3] с.21-42	6
3	Дослідження параметрів вимірювальних генераторів та частотомірів Літ.: [2] с.41-46	6
4	Дослідження вимірювальних можливостей універсальних осцилографів Літ.: [2] с.23-30; [3] с.21-32	6
5	Робота з мультиметром, вольтметром і амперметром. Вимірювання параметрів сигналів і компонентів Літ.: [8] с.89-119	6
6	Побудова структурних і функціональних схем електронних пристроїв і систем у відповідності до вимог державних стандартів Літ.: [14] ; [17] с.101-106; [20] ; [21]	6
7	Розробка схем електричних принципів у відповідності до вимог державних стандартів Літ.: [14] ; [17] с.101-106; [20] ; [21]	6
8	Оформлення супровідної документації до схем електричних вузлів у відповідності до вимог державних стандартів Літ.: [14] ; [17] с.101-106; [20] ; [21]	6
9	Підсумкове заняття, тестування	6
<b>Разом:</b>		<b>54</b>

### Зміст самостійної (у т.ч. індивідуальної) роботи

На самостійне опрацювання студентів виноситься опрацювання лекційного матеріалу, підготовка до практичних занять, підготовка до контрольної роботи. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу, підготовка до ЛР 1	15
2	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 1, підготовка до ЛР 2	17
3	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 2, підготовка до ЛР 3	17
4	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 3, підготовка до ЛР 4	17
5	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 4, підготовка до ЛР 5	17
6	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 5, підготовка до ЛР 6	17
7	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 6, підготовка до ЛР 7	17
8	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 7, підготовка до ЛР 8	17
9	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 8, підготовка до тестування	16
<b>Разом:</b>		<b>150</b>

**Умовні позначення:** ЛР – лабораторна робота

## **ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ**

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції з використанням словесних, наочних та інтерактивних методів і візуалізації (лекції); лабораторні роботи з використанням практичних, проблемних, продуктивних методів, тренінгових майстер-класів, самостійна робота передбачає пояснювально-ілюстративні та дослідницькі методи.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини лабораторних робіт передбачає роботу у малих групах з призначенням тим-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність складу робочих груп між лабораторними роботами сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; спілкування з проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів; обмежений час на виконання лабораторних робіт і тестових завдань, чітко визначені терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

## **МЕТОДИ КОНТРОЛЮ**

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- тестування.

При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).



## ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості.

### Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

Аудиторна робота		Контрольні заходи	Підсумковий контрольний захід
Лабораторні роботи №:	Тестовий контроль 1	Тестовий контроль 2	Семестровий контроль
1 - 8	Т 1-3	Т 4-7	Залік
ВК: 0,8	0,2	0,2	

**Оцінювання лабораторних робіт.** Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

**Оцінювання тестових завдань.** Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

### Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

### Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	2
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; вміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві-три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ECTS встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

**Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС**

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання		
A	4,75–5,00	5	Зараховано	<b>Відмінно</b> – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		<b>Добре</b> – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		<b>Добре</b> – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		<b>Задовільно</b> – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		<b>Задовільно</b> – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незараховано	<b>Незадовільно</b> – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		<b>Незадовільно</b> – необхідна серйозна подальша робота і повторне вивчення дисципліни

**ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ  
ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ**

1. Взаємозв'язок метрологія-стандартизація-сертифікація.
2. Метрологія: основні поняття та визначення.
3. Види фізичних величин.
4. Міжнародна система одиниць.
5. Основні одиниці системи СІ.
6. Похідні та позасистемні одиниці системи СІ.
7. Кратні та частинні одиниці системи СІ.
8. Призначення і загальна класифікація вимірювальних засобів.
9. Класифікація електронних вимірювальних приладів.
10. Групи, підгрупи і шифри типів електронних вимірювальних приладів.
11. Характеристики вимірювальних приладів.
12. Вимоги до сучасних вимірювальних приладів.
13. Вимірювання як метрологічний процес.
14. Стандартизовані визначення характеристик вимірювань.
15. Методи вимірювань.
16. Фактори, що впливають на точність вимірювань.
17. Похибки – поняття та класифікація.
18. Нормативно-правова база метрології.
19. Державна метрологічна система України.
20. Міжнародні метрологічні організації.
21. Система забезпечення єдності вимірювань.
22. Поняття, задачі, рівні стандартизації
23. Нормативні документи державної стандартизації
24. Органи державної стандартизації України
25. Органи міжнародної стандартизації
26. Система стандартизації країн ЄС
27. Єдина система конструкторської документації (ЄСКД) - основні поняття, визначення та призначення (ДСТУ ГОСТ 2.001:2006).
28. Сфера поширення стандартів ЄСКД.
29. Склад, класифікація й позначення стандартів ЄСКД.
30. Види конструкторських документів (ДСТУ 3321:2003).
31. Комплектність конструкторських документів.
32. Загальні правила оформлення графічних і текстових документів за ЄСКД.
33. Основні надписи конструкторських документів за ЄСКД.
34. Етапи розробки конструкторської документації за ЄСКД.
35. Загальні вимоги до текстових документів (ГОСТ 2.105-95).
36. Оформлення пояснювальної записки за ЄСКД.
37. Порядок викладення тексту документів за ЄСКД.
38. Правила написання позначень і найменувань одиниць фізичних величин за ЄСКД.
39. Оформлення ілюстрацій і додатків за ЄСКД.
40. Побудова таблиць за ЄСКД.
41. Оформлення списку літератури за ЄСКД.
42. Оформлення специфікації за ЄСКД.
43. Єдина система програмної документації (ЄСПД).
44. Види графічних документів за ЄСКД.
45. Правила нанесення розмірів за ЄСКД.
46. Загальні вимоги до робочих креслень за ЄСКД.
47. Креслення деталей за ЄСКД.
48. Креслення складальні за ЄСКД.
49. Креслення загального виду за ЄСКД.
50. Різновиди схем і загальні вимоги до їх виконання за ЄСКД.
51. Схеми електричні структурні за ЄСКД.

52. Схеми електричні функціональні за ЄСКД.
53. Схеми електричні принципів за ЄСКД.
54. Схеми з'єднань за ЄСКД.
55. Початок стандартизації в інформаційній безпеці.
56. Критерії безпеки комп'ютерних систем міністерства оборони США TCSEC – базові положення.
57. Розвиток стандартів інформаційної і кібербезпеки – характерні тенденції.
58. Міжнародні стандарти для системи управління інформаційною безпекою ISO 270xx – роль в стандартизації питань інформаційної і кібербезпеки.
59. Стандарт ISO 27001 – роль і призначення.
60. Сертифікація – основні поняття і визначення.
61. Види сертифікації.
62. Загальні принципи сертифікації.
63. Система сертифікації.
64. Норми і правила сертифікації.
65. Акредитація органів сертифікації.
66. Сертифікація систем управління інформаційною безпекою.
67. Міжнародна сертифікація фахівців в галузі інформаційної безпеки.

## МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Побудова захищених комп'ютерних систем” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

### РЕКОМЕНДОВАНА ЛІТЕРАТУРА

#### Основна

1. Козюра В.Д., Хорошко В.О., Шелест М.С., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
3. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
4. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека. К.: ДУТ, 2015. 288 с.
5. Грабар І. Г., Гришук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир: ЖНАЕУ, 2019. 280 с.
6. Інформаційна безпека: навч. посіб./Бобало Ю. Я. та ін.; за заг. ред. д-ра техн. наук, проф. Бобала Ю. Я. та д-ра техн. наук, доц. Горбатого І. В. Львів: В-во Львівської політехніки, 2019. 580 с.
7. Бибка О.І. Конспект лекцій з дисципліни „Автоматизація адміністрування мережної інфраструктури”. Харків: ХНУРЕ, 2020. 51с.
8. Архипова, Е., & Гудела, М. Modern trends in the formation of the corporate communication system in public authorities. SWorldJournal. 2020. №3(06-03), P. 75–83. URL: <https://doi.org/10.30888/2663-5712.2020-06-03-028>
9. Федотова-Півень І. М., Миронець І. В., Півень О. Б., Сисоєнко С. В., Миронюк Т. В.; за ред. В. М. Рудницького. Операційні системи: навч. посіб. Харків: ТОВ «ДІСА ПЛЮС», 2019. 216с.
10. Жаровський Р.О. Захист інформації у комп'ютерних системах: конспект. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
11. Sokolov V. Y., Kurbanmuradov, D. M. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2018. №1(1). С. 6–16. <https://doi.org/10.28925/2663-4023.2018.1.616>
12. Олександр Мізюк. Системи числення. URL: <https://nrs.rozh2sch.org.ua/>

#### Додаткова

13. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
14. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
15. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
16. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
17. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
19. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.
20. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Чинний від 2016-27-12. Київ: ДП «УкрНДНЦ», 2018. 50 с.
21. Барабаш О. В., Гришук Р. В., Молодецька-Гринчук К. В. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів. Наукоємні технології. 2018. № 2 (38). С. 232–239. URL: <http://jrn1.nau.edu.ua/index.php/SBT/article/view/12855>

22. Молодецька К. В. Механізми синергетично керованої самоорганізації акторів у соціальних інтернет-сервісах. Управління розвитком. 2018. Т. 4, вип. 4. С. 1–13. Режим доступу: <http://ir.znau.edu.ua/handle/123456789/9582>
23. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. Third edition. Burlington :Jones & Bartlett Learning, 2018. 571 p.
24. Peter Dordal, Loyola. An Introduction to Computer Networks. Independent, 2020. 886с.
25. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. Київ: Київ. нац. торг.-екон. ун-т, 2020. 101 с.
26. Основні правила кібергігієни. URL: <https://cert.gov.ua/recommendation/31> Дата звернення 15.07.2023:
27. Gursev Singh Kalra. "Threat analysis of an enterprise messaging system". URL: <https://www.sciencedirect.com/science/article/abs/pii/S1353485814701217#preview-section-abstract>
28. Gerardus Blokdyk. (2019). Secure Messaging: A Complete Guide. Inc. ISBN: 0655820469. 480 p.
29. National Institute of Standards and Technology. (2017). An Introduction to Information Security. Special Publication 800-12r1. 101 p. Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>
30. The Art of Service - Virtual Machines Publishing. (2021). Virtual Machines: A Complete Guide. Packt Publishing. ISBN: 186743556X. 500 p.
31. Захист від шкідливих програм і відновлення та резервування даних
32. Peter Dordal. An Introduction to Computer Networks. Loyola. Independent, 2020. 886с.
33. S. Gokulakrishnan and J. M. Gnanasekar, "Data integrity and recoverymanagement under peer-to-peer convoluted fault recognition cloud sys-tems," Journal of Computational and Theoretical Nanoscience, vol. 17,no. 5, pp. 2147–2150, 2020.
34. FreeVacy. (2023). Resources. URL: <https://www.freevacy.com/resources>
35. Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брендмауерів
36. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
37. LazyAdmin, (2020) Home Network Security. URL: <https://lazyadmin.nl/home-network/home-network-security>
38. National Security Agency. (2022). Network Infrastructure Security Guide. URL: [https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR\\_NSA\\_NETWORK\\_INFRASTRUCTURE\\_SECURITY\\_GUIDE\\_20220615](https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615)
39. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." ACM Computing Surveys (CSUR) 54.3 (2021): 1-36.
40. Безпечна робота із соціальними інтернет сервісами та інструменти виявлення неправдивих повідомлень
41. Zhou, X., & Zafarani, R. (2020). A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. ACM Computing Surveys, 53(5), 1–40.
42. Social Engineering. URL: <https://www.imperva.com/learn/application-security/social-engineering-attack/>
43. Gardner, B. (2018). Social Engineering in Non-Linear Warfare. Journal of Applied Digital Evidence, 1(1). [Електронний ресурс]. – Режим доступу : <http://mds.marshall.edu/jade/vol1/iss1/1>

## ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE. Доступ до ресурсу: <https://msn.khmnu.edu.ua/>.
2. Електронна бібліотека університету. Доступ до ресурсу: <http://library.khmnu.edu.ua/>.