**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ**

**ННІ «ДНІПРОВСЬКИЙ МЕТАЛУРГІЙНИЙ ІНСТИТУТ»**

**ФАКУЛЬТЕТ ЯКОСТІ ТА ІНЖЕНЕРІЇ МАТЕРІАЛІВ**

**КАФЕДРА СИСТЕМ ЯКОСТІ, СТАНДАРТИЗАЦІЇ ТА МЕТРОЛОГІЇ**

**ЗАТВЕРДЖУЮ**
Перший проректор УДУНТ
Проф. _____ Анатолій РАДКЕВИЧ
"27" 08 2024 р.

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ЗА СТАНДАРТАМИ ISO СЕРІЇ 27000)

Рівень вищої освіти: **перший (бакалаврський)**

Спеціальність: **175 - Інформаційно-вимірювальні технології**

Освітня програма: **Інформаційно-вимірювальні технології та інженерія якості**

Статус дисципліни: **обов'язкова**

Обсяг дисципліни: **4 кредити ЄКТС**

Код освітньої компоненти: **ОК 2.19**

Мова викладання: **українська**

Дніпро – 2024

Робоча програма навчальної дисципліни «Основи інформаційної безпеки (за стандартами ISO серії 27000)»

Розробив:

професор, д.т.н. професор _____ Анатолій ДОЛЖАНСЬКИЙ

Протокол засідання Групи забезпечення якості освітньої програми «Інформаційно-вимірювальні технології та інженерія якості»
від «07» червня 2024 р., № 7.

Гарант освітньої програми: _____ Євген ЧЕРНЕЦЬКИЙ

ПОГОДЖЕНО
Навчально-методичний відділ _____ Олена ЗАХАРОВА

«25» червня 2024 р.

ПОГОДЖЕНО
Заст. керівника навчального
відділу УДУНТ _____ Тетяна ШЕМЕТ

«25» червня 2024 р.

ЗАТВЕРДЖЕНО
Протокол засідання кафедри Систем якості, стандартизації та метрології
від «26» червня 2024 р., № 12.
Завідувач кафедри: _____ Анатолій ДОЛЖАНСЬКИЙ

«26» червня 2024 р.

Реєстраційний номер 175.1.02.ОК2.19-24

# 1 МІСЦЕ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ В ОСВІТНІЙ ПРОГРАМІ

## 1.1 Мета навчальної дисципліни

Мета викладання навчальної дисципліни – ознайомлення студентів із сучасними підходами, методиками, засобами та пристроями для захисту інформаційно-комп'ютерних систем і персональної інформації користувача, здебільшого, на основі стандартів ISO серії 27000; навчити студентів спеціалізованим заходам у сфері інформаційної та комп'ютерної безпеки, які сприяють захисту сучасних систем менеджменту інформаційної безпеки (СМІБ) у професійній діяльності, що пов'язана із отриманням, обробкою, накопиченням і захистом особистої, службової тощо інформації.

## 1.2 Компетентності, формування яких забезпечується

Навчальна дисципліна забезпечує набуття таких передбачених освітньою програмою компетентностей:

ІК1. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми метрології та інформаційно-вимірювальної техніки, які характеризуються комплексністю та невизначеністю умов, що передбачає застосування теорій та методів метрології, способів побудови засобів автоматизації та приладобудування, включаючи системи, інформаційних технологій як у сфері проектування виробів приладобудування, так і при опрацюванні вимірювальної інформації в ситуаціях, що характеризуються невизначеністю умов і вимог.

ЗК-1. Здатність застосовувати професійні знання й уміння у практичних ситуаціях.

ЗК-4. Навички використання інформаційних і комунікаційних технологій.

ЗК-5. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.

ЗК-6. Навички здійснення безпечної діяльності.

ЗК-10. Здатність приймати обґрунтовані рішення, оцінювати та забезпечувати якість виконуваних робіт, працювати як індивідуально, так і в команді.

ФК-11 Здатність розуміти та використовувати світову технічну документацію, зокрема, міжнародні, регіональні та міждержавні стандарти і рекомендації та настанови за спеціальністю.

## 1.3 Програмні результати навчання, що забезпечуються

Відповідно до освітньої програми дисципліна спільно з іншими освітніми компонентами має забезпечити досягнення таких програмних результатів навчання:

ПРН-1. Вміти знаходити обґрунтовані рішення при складанні

структурної, функціональної та принципової схем засобів інформаційно-вимірювальної техніки.

ПРН-4. Вміти вибирати, виходячи з технічної задачі, стандартизований метод оцінювання та вимірювального контролю характерних властивостей продукції та параметрів технологічних процесів.

ПРН-9. Розуміти застосовуванні методики та методи аналізу, проєктування і дослідження, а також обмежень їх використання у конкретних умовах.

ПРН-13. Знати та вміти застосовувати сучасні інформаційні технології для розв'язання задач у сферах метрології, інформаційно-вимірювальної техніки та забезпечення якості.

У результаті вивчення дисципліни студент повинен:

***знати:***

• предмет, мету вивчення, завдання і значення курсу;

• основні загрози безпеки;

• теоретичні основи інформаційної безпеки, в тому числі її нормативно-правове забезпечення;

• основні характеристики апаратних засобів захисту інформації;

• шляхи захисту комп'ютерної інформації в операційних системах;

• особливості програмних засобів, що містять небезпеку;

• підходи до формування криптографічних методів захисту інформації;

• способи убезпечення комп'ютерних мереж;

• підходи до захисту інформації в глобальних і хмарних мережах;

• перелік і характеристику основних стандартів щодо інформаційної безпеки;

• місце інформаційної безпеки в системі національної безпеки України;

***уміти:***

• аналізувати інформаційні загрози та обирати засоби щодо протидіям порушників;

• визначати шляхи із захисту інформації в комп'ютерних системах.

### 1.4 Міждисциплінарні зв'язки

Навчальна дисципліна є обов'язковою для вивчення студентами, які здобувають освітній ступінь бакалавра за Освітньою програмою «Інформаційно-вимірювальні технології та інженерія якості (за стандартами ISO серії 27000».

Опануванню дисципліни передує вивчення дисциплін циклу загальної підготовки («Іноземна мова за професійним спрямуванням», «Правознавство», «Філософія» та ін.), дисциплін циклу фахової підготовки («Методи та засоби вимірювань та контролю», «Програмне забезпечення інформаційно-вимірювальних технологій», «Основи системного аналізу» та ін.).

Набуті знання і вміння застосовуються при опануванні програми підготовки бакалаврів за фахом, при підготовці ними випускної роботи та у майбутній професійній діяльності.

## 2 ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ ЗА НАВЧАЛЬНОЮ

**ДИСЦИПЛІНОЮ**

| Код | Очікуваний результат навчання | Рівень |
|---|---|---|
| ОРН-1 | Розуміти, поясняти та класифікувати підходи, методики, засоби та пристрої для захисту інформаційно-комп'ютерних систем і персональної інформації користувача. | II |
| ОРН-2 | Вміти використовувати знання щодо теоретичних основ інформаційної безпеки, в тому числі її нормативно-правове забезпечення, характеристик апаратних засобів та шляхів захисту інформації. | III |
| ОРН-3 | Використовувати розроблені методичні та нормативні документи, що стосуються підходів до захисту інформації в глобальних і хмарних мережах. | IV |
| ОРН-4 | Перевіряти СМІБ у цілому та окремі її елементи на відповідність вимогам нормативних документів та стейкхолдерів. | VI |

Соціальні навички (soft skills),
розвитку яких сприяє навчальна дисципліна

| Код | Соціальна навичка (*soft skill*) |
|---|---|
| ОН1 | Здатність управляти власним часом. |
| ОН2 | Здатність самостійно приймати рішення. |
| ОН3 | Здатність формулювати цілі. |
| ОН4 | Прихильність до позитивного мислення з розумінням важливості предмету вивчення як філософії забезпечення загальної якості інформаці та інформаційних систем. |
| КН1 | Здатність зрозуміло формулювати думки. |
| КН3 | Здатність дискутувати та надавати аргументовані відповіді з використанням спеціальних загальноприйнятих термінів. |
| УН1 | Здатність працювати в команді. |

## 3 **РОЗПОДІЛ ГОДИН ЗА ВИДАМИ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ**

Денна форма освіти

| Види навчальної діяльності | Усього | Семестри/півсеместри | | | |
|---|---|---|---|---|---|
| | | 5 | | 6 | |
| | | 5/9 | 5/10 | 6/11 | 6/12 |
| Усього годин за навчальним планом | 120 | | - | - | 120 |
| у тому числі: Аудиторні заняття | 48 | | - | - | 48 |
| Лекції | 32 | | | | 32 |
| – практичні заняття | 16 | | - | - | 16 |
| – лабораторні роботи | - | | - | - | - |
| – семінарські заняття | - | | - | - | - |
| ***Самостійна робота*** | 72 | | - | - | 72 |
| – підготовка до аудиторних занять | 24 | | - | - | 24 |
| – виконання та захист курсової роботи | - | | - | - | - |
| – виконання та захист індивідуальних завдань | - | | - | - | - |
| – підготовка та складання екзаменів | - | | - | - | - |
| – підготовка до інших контрольних заходів | 24 | | - | - | 24 |
| – опрацювання розділів, які не викладаються на лекціях | 24 | | - | - | 24 |
| ***Форма семестрового контролю*** | Диф. залік | | - | | Диф. залік |

Заочна форма освіти

| Види навчальної діяльності | Усього | Семестри | |
|---|---|---|---|
| | | 5 | 6 |
| Усього годин за навчальним планом | 120 | | 120 |
| у тому числі: ***Аудиторні заняття*** | 12 | | 12 |
| – лекції | 8 | | 8 |
| – практичні заняття | 4 | | 4 |
| – лабораторні роботи | - | | - |
| – семінарські заняття | - | | - |
| ***Самостійна робота*** | 108 | | 108 |
| – підготовка до аудиторних занять | 6 | | 6 |
| – виконання та захист курсової роботи | - | | - |
| – виконання та захист індивідуальних завдань | 12 | | 12 |
| – опрацювання навчального матеріалу | 66 | | 66 |
| – підготовка та складання екзаменів | - | | - |
| – підготовка та складання інших контрольних заходів | 24 | | 24 |
| ***Форма семестрового контролю*** | Диф. залік | | Диф. залік |

# 4 ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| Роз-діл | Тема лекції (заняття) | Обсяг, годин | | ОРН | СН |
|---|---|---|---|---|---|
| | | Очна форма | Заочна форма | | |
| I | **Розділ 1. Базові положення інформаційної безпеки** | | | ОРН-1<br>ОРН-2 | ОН1<br>ОН2<br>ОН4<br>КН3<br>КН1 |
| | ***Лекції:***<br>**Лекція 1. Вступ. Основні поняття і визначення.** Зв'язок інформації з діяльністю суспільства. Державна політика України із захисту інформації. | 4 | 1 | | |
| | **Лекція 2. Розповсюдження та уразливість інформації.** Канали руху, обробка, загрози та концепція захисту інформації. | 4 | 1 | | |
| | ***Практичні заняття:***<br>**Практична робота №1.** Аналіз змісту стандартів ISO/IEC 17799 та EN ISO/IEC 27001 щодо базових положень інформаційної безпеки | 4 | 1 | | |
| | ***Самостійна робота:*** | | | | |
| | Підготовка до аудиторних занять | 6 | 1,5 | | |
| | Виконання та захист індивідуальних завдань | - | - | | |
| | Опрацювання розділів програми, які не викладаються на лекціях (для очного навчання): Методи захисту. Інформаційна безпека у взаємовідносинах з постачальниками. Частина 1. Огляд і концепція (ISO/IEC 27036-1:2014, IDT) | 6 | - | | |
| | Опрацювання навчального матеріалу (для заочного навчання)<br>Методи захисту. Інформаційна безпека у взаємовідносинах з постачальниками. Частина 1. Огляд і концепція (ISO/IEC 27036-1, 2, 3, 4:2014, IDT); | - | 19,5 | | |
| | Підготовка та складання інших контрольних заходів | 6 | 6 | | |
| | У с ь о г о: | 30 | 30 | | |
| II | **Розділ 2. Складові інформаційної безпеки** | | | ОРН-2<br>ОРН-3<br>ОРН-4 | ОН1<br>ОН4<br>КН1<br>КН3 |
| | ***Лекції:***<br>**Лекція 3. Концепції та моделі інформаційної безпеки.** Керування безпекою інформаційних технологій. Архітектура інформаційної безпеки. | 4 | 1 | | |
| | **Лекція 4. Основні загрози для безпечності інформації.** Загрози доступності та конфіденційності. Шкідливе програмне забезпечення. Загрози цілісності. | 4 | 1 | | |
| | ***Практичні заняття:***<br>**Практична робота № 2. Аналіз положень стандартів EN ISO/IEC 27003 та ISO/IEC 27013:2021 щодо складових інформаційної безпеки** | 4 | 1 | | |

| | | | | | |
|---|---|---|---|---|---|
| | ***Самостійна робота:*** | | | | |
| | Підготовка до аудиторних занять | 6 | 1,5 | | |
| | Виконання та захист індивідуальних завдань | - | - | | |
| | Опрацювання розділів програми, які не викладаються на лекціях (для очного навчання): Кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT) | 6 | - | | |
| | Опрацювання навчального матеріалу (для заочного навчання) Кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT) | - | 19,5 | | |
| | Підготовка та складання інших контрольних заходів | 6 | 6 | | |
| | У с ь о г о: | 30 | 30 | | |
| III | **Розділ 3. Заходи із захисту інформації** | | | ОРН-1 ОРН-2 ОРН-3 ОРН-4 | ОН1 ОН2 ОН3 ОН4 КН1 КН3 УН1 |
| | ***Лекції:*** **Лекція 5. Ідентифікація та аутентифікація користувачів, керування доступом до інформації.** Керування персоналом. Створення режиму доступу і безпеки на підприємстві. Криптографічний та програмно-технічний захист інформації. | 4 | 1 | | |
| | **Лекція 6. Контроль цілісності інформації.** Керування безпекою інформаційних технологій. Захист інформації в комп'ютерних та глобальних мережах. | 4 | 1 | | |
| | ***Практичні заняття:*** **Практична робота № 3. Аналіз положень стандартів EN ISO/IEC 27032, та ISO/IEC 27033 та ISO/IEC 27034-1,2 щодо кібербезпеки, захисту мережі та захисту прикладних програм** | 4 | 1 | | |
| | ***Самостійна робота:*** | | | | |
| | Підготовка до аудиторних занять | 6 | 1,5 | | |
| | | | | | |
| | Аналіз положень стандарту (EN ISO/IEC 27043:2016 «Принципи і процеси розслідування інцидентів» | 6 | - | | |
| | Опрацювання навчального матеріалу (для заочного навчання) Аналіз положень стандартів (EN ISO/IEC 27043:2016; ДСТУ ISO/IEC 27042:2015 «Принципи і процеси розслідування інцидентів»; Аналіз та інтерпретація цифрового доказу (IDT) | - | 19,5 | | |
| | Підготовка та складання інших контрольних заходів | 6 | 6 | | |
| | У с ь о г о: | 30 | 30 | | |

| | | | | | |
|---|---|---|---|---|---|
| IV | **Розділ 4. Аудит і управління ризиками при захисті інформації** | | | ОРН-1<br>ОРН-2<br>ОРН-3<br>ОРН-4 | ОН1<br>ОН2<br>ОН3<br>ОН4<br>КН1<br>КН3<br>УН1 |
| | ***Лекції:*** | 30 | 30 | | |
| | **Лекція 7. Аудит захищеності інформації**. Проведення аудиту та протоколювання**.** | 4 | 1 | | |
| | **Лекція 8. Управління ризиками при захисті інформації.** Оцінювання загроз, вразливостей і ризиків. | 4 | 1 | | |
| | ***Практичні заняття:*** | | | | |
| | **Практична робота № 4. Аналіз положень стандартів ISO/IEC 27005, EN ISO/IEC 27006 та** EN **ISO/IEC 27007 щодо аудиту, оцінювання та управління ризиками системи інформаційної безпеки** | 4 | 1 | | |
| | **Самостійна робота:** | | | | |
| | Підготовка до аудиторних занять | 6 | 1,5 | | |
| | Виконання та захист індивідуальних завдань<br>Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT); Інформаційні технології. Методи захисту; Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII (ISO/IEC 27018:2019, IDT) | - | 12 | | |
| | Опрацювання розділів програми, які не викладаються на лекціях (для очного навчання):<br>Аналіз положень стандарту ISO/IEC 27004:2016 «Системи управління інформаційною безпекою»; Моніторинг, вимірювання, аналіз та оцінка (ISO/IEC TS 27008:2019)» | 6 | - | | |
| | Опрацювання навчального матеріалу (для заочного навчання)<br>Аналіз положень стандарту ISO/IEC 27004:2016 «Системи управління інформаційною безпекою» та Технічної специфікації оцінювання захисту інформаційної безпеки ISO/IEC TS 27008:2019<br>«Моніторинг, вимірювання, аналіз та оцінка»; | - | 7,5 | | |
| | Підготовка та складання інших контрольних заходів | 6 | | | |
| | Усього: | 30 | 30 | | |

## 5 МЕТОДИ ВИКЛАДАННЯ ТА НАВЧАННЯ

Дисципліна передбачає навчання через:

– пояснювальні вербально-ілюстративні інтерактивні лекції (МН1);

– репродуктивно-практичні заняття (МН2);

– практико-орієнтоване навчання (МН3);

– частково-пошукове навчання (МН4);

– модульне навчання (МН5);

– проблемне навчання (МН6).

*Лекції* надають студентам матеріали з теорії та методології забезпечення інформаційної безпеки на основі відповідних (міжнародних, регіональних і національних нормативних документів (стандартів) та відомих позитивних результатів впровадження відповідних систем безпеки інформації, що є основою для самостійного удосконалення компетентностей здобувачів вищої освіти.

Лекції проводяться в інтерактивному режимі з розглядом при представленні викладачем навчальної інформації у ході дискусії з проблемних ситуацій.

Лекції доповнюються репродуктивно-практичними заняттями, які мають ділову спрямованість (часто – за вибором здобувача згідно з предметною сферою будь-якої економічної діяльності: важка, легка або хімічна промисловість, будівництво, бізнес, менеджмент, транспорт, виробництво харчової продукції, фармакологія тощо.

*Практико-орієнтоване навчання* реалізується шляхом самостійного визначення здобувачем освіти предметної сфери для розробки складових інформаційної безпеки (на підставі власного досвіду та/або інформації, що отримана з різних джерел) при виконанні ним практичних робіт. Цей метод застосовується на практичних заняттях із засвоєння основних положень на основі відомих принципів та підходів з інформаційної безпеки діяльності при забезпечення якості продукції, процесів та систем, наприклад, коли викладач пропонує матрицю відображення результатів аналізу за певними критеріями, а здобувачі, враховуючи надані критерії, відображують їх за власним обраним варіантом.

*Пошуковий метод* застосовується через організацію активного розв'язання завдань, висунутих викладачем, та практичних робіт, які характеризується наперед неповністю визначеною предметною сферою щодо розробки складових системи інформаційної безпеки та частково мають творчу спрямованість.

*Модульне навчання* полягає у представленні навчального матеріалу у вигляді окремих змістовно, методично і організаційно завершених розділів (модулів): автономних частин дисципліни, що інтегруються з іншими частинами.

Заходи, що використовуються для *розвитку соціальних навичок*:

1) Здатність керувати власним часом (ОН1) формується встановленням контрольних термінів виконання практичних робіт, самостійної роботи і, додатково - для студентів заочної форми навчання - при виконанні ними індивідуального завдання.

2) Здатність самостійно приймати рішення (ОН2) реалізується завдяки необхідності застосування способів з виконання студентами практичних робіт, самостійної роботи і, додатково – для студентів заочної форми навчання - індивідуального завдання.

3) Здатність формулювати цілі (ОН3) формується під час цілеспрямованої розробки (в рамках ділової гри) складових системи інформаційної безпеки у відповідності з певними вимогами нормативних документів (застосовних відповідних стандартів).

4) Для розвитку прихильності до позитивного мислення (ОН4) лектор проявляє доброзичливе ставлення до студентів, наводить приклади успішного використання систем інформаційної безпеки, виконання вимог навчального плану за Освітньою програмою та застосування набутих знань і умінь у виробничій діяльності випускників.

5) Здатність зрозуміло письмово відображувати думки (КН1) формується у процесі формулювання висновків за результатами робіт і, додатково – для студентів заочної форми навчання - індивідуального завдання.

6) Здатність надавати аргументовані відповіді (КН3) розвивається у студентів під час опитувань на аудиторних заняттях, а для студентів заочної форми навчання при захисті індивідуального завдання.

7) Здатність результативно працювати у команді (УН1) розвивається у студентів при обговоренні ними (в рамках ділової гри) потрібних складових системи інформаційної безпеки у конкретних умовах.

# 6 МЕТОДИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

## 6.1 Методи поточного оцінювання

За дисципліною передбачені такі методи поточного оцінювання: опитування та усні коментарі викладача за результатами інтерактивного спілкування, самооцінювання, обговорення та взаємне оцінювання студентами результатів виконання практичних робіт та індивідуального завдання (останнє - для студентів заочної форми навчання).

## 6.2 Методи та критерії семестрового оцінювання

Оцінки з кожного розділу визначаються за шкалою, шо прийнята в університеті згідно із затвердженими критеріями за результатами таких контрольних заходів:

– оцінки РО1, РО2, РО 3 та РО 4 з розділів 1, 2, 3 та 4 відповідно – за результатами письмової контрольної роботи у тестовій формі (РК1).

## 6.3 Критерії семестрового та підсумкового оцінювання

Формою семестрового контролю з дисципліни є диференційований залік.

Семестрова оцінка формується як середнє арифметичне оцінок РО1, РО2, РО3 та РО4 з округленням до найближчого цілого числа.

Необхідною умовою отримання позитивної оцінки з розділів 1, 2, 3 та 4 є відпрацювання та надання звіту з усіх практичних робіт відповідного розділу.

Обов'язковою умовою для обчислення оцінки диференційованого заліку є наявність позитивних оцінок з усіх розділів.

Необхідною умовою отримання позитивної семестрової оцінки з дисципліни за заочною формою навчання є зарахування індивідуального завдання, за яке відповідно до затверджених критеріїв виставляється оцінка «зараховано» / «не зараховано».

Підсумкова оцінка навчальної дисципліни дорівнює семестровій оцінці.

## 7 РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

### 7.1 Засоби навчання

Навчальний процес передбачає використання графічних засобів: схеми, плакати, копії документів тощо (ЗН1), комп'ютеризованих робочих місць для проведення інтерактивних лекцій, практичних робіт (ЗН2).

### 7.2 Інформаційне та навчально-методичне забезпечення

***Основна література***


1. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2018. 316 с.

2. Вишня В. Б., Гавриш, О. С. Рижков Е.В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

3. Стандарти інформаційної безпеки ISO/EN ISO/ ДСТУ EN ISO серії 27000.

2. Закон України «Про державну таємницю» від 21 січня 1994 року, N 3855-XII (зі змінами та доповненнями у наступні роки.


***Інформаційні ресурси в Інтернеті***

| | |
|---|---|
| 1. rada.kiev.ua | Верховна Рада. Законодавство України. Проєкти НД. Органи виконавчої влади. |
| 2. http: uas.org.ua | Державне підприємство «УкрНДНЦ» - Національний орган стандартизації |
| 3. leonorm.lviv.ua | Інформаційний сервер НІЦ «Леонорм» стосовно інформації щодо технічного регулювання, виробництва та реалізації продукції |
| 4. iso.org | Сайт Міжнародної організації із стандартизації |
| 5. cen.eu | Європейський комітет із стандартизації. Офіційний сайт. |

## 8 УЗГОДЖЕННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ З МЕТОДАМИ ВИКЛАДАННЯ, НАВЧАННЯ ТА ОЦІНЮВАННЯ

| Очікуваний результат навчання за дисципліною | Програмні результати навчання | Види навчальних занять*) | Методи, викладання і навчання | Засоби навчання | Форми та методи оцінювання |
|---|---|---|---|---|---|
| ОРН-1 | ПРН-1 | Л, ПЗ | МН1, МН2, МН3, МН4, МН5 | ЗН1, ЗН2 | РК1 |
| ОРН-2 | ПРН-4, ПРН-9 | Л, ПЗ | МН1, МН2, МН3, МН4, МН5 | ЗН1, ЗН2 | РК1 |
| ОРН-3 | ПРН-3, ПРН-9, ПРН-13 ПРН-16 | Л, ПЗ | МН1, МН2, МН3, МН4, МН5 | ЗН1, ЗН2 | РК1 |
| ОРН-4 | ПРН-01, ПРН-4, ПРН-9 ПРН-13 | Л, ПЗ | МН1, МН2, МН3, МН4, МН5, МН6 | ЗН1, ЗН2 | РК1 |

***) Примітка:** Л – лекції; ПЗ – практичні заняття