МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

ОРГАНІЗАЦІЯ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ

робоча програма навчальної дисципліни

Галузь знань	***12 "Інформаційні технології"***
Спеціальність	***125 "Кібербезпека"***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри менеджменту,
логістики та економіки Олена ЯСТРЕМСЬКА

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *менеджменту, логістики та економіки*
Протокол № 2 від 27.08.2020 р.

Розробник:
Томах В. В., к. е. н., доцент кафедри менеджменту, логістики та економіки

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Навчальна дисципліна “Організація та інформаційне забезпечення управлінської діяльності” є базовою навчальною дисципліною та вивчається згідно з навчальним планом підготовки фахівців освітнього ступеню "бакалавр" спеціальність 125 «Кібербезпека» галузі знань 12 "Інформаційні технології". Сучасні економічні умови, в яких функціонують суб’єкти господарювання, характеризуються високим рівнем динамічності. Це сприяє актуалізації питань інформаційного забезпечення управлінської діяльності у всіх сферах. В швидкоплинних умовах ведення бізнесу особливо важливим є вміння прийняття якісних науково обґрунтованих управлінських рішень, що є можливим тільки за умови якісного організаційного та інформаційного забезпечення особи, що приймає рішення. У таких умовах важливості набуває вміння керівників адаптувати класичні та розробляти нові підходи до організаційного та інформаційного забезпечення управлінської діяльності. Ґрунтовна фахова підготовка студентів дозволить сформувати у майбутніх фахівців необхідні компетентності для створення якісних умов організаційних та інформаційних умов управлінської діяльності.

Подано тематичний план навчальної дисципліни та її зміст за модулями і темами. Вміщено плани лекцій і лабораторних робіт, матеріал щодо закріплення знань (самостійну роботу, контрольні запитання), критерії оцінювання знань студентів, професійні компетентності, якими повинен володіти студент після вивчення дисципліни.

Мета навчальної дисципліни: формування у студентів необхідних компетентностей з організації та інформаційного забезпечення управлінської діяльності, необхідних для їх майбутньої професійної діяльності.

Характеристика навчальної дисципліни

Курс	**3**
Семестр	**2**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**Екзамен**

Структурно-логічна схема вивчення навчальної дисципліни:

	Постреквізити
Базові знання з предметів середньої освіти, Менеджмент інформаційної безпеки	Організаційне забезпечення захисту інформації

Компетентності та результати навчання за дисципліною

Компетентності	**Результати навчання**
КФ 1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	РН-7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН-8 готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС)

	організації (підприємства) відповідно до вимог нормативно-правових документів; РН-33 вирішувати задачі забезпечення безпере-вності бізнес процесів організації на основі теорії ризиків; РН-34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН-35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН-44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН-24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН-27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН-29 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН-32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

	РН-33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН-34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН-35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН-42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН-44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН-45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН-46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	РН-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-21 вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН-24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформацій-них та інформаційно-телекомунікаційних (автома-тизованих) системах на основі моделей управлінь-ня доступом (мандатних, дискреційних, рольових); РН-25 забезпечувати введення підзвітності системи уп-равління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформа-ційно-телекомунікаційних (автоматизованих) си-стемах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН-28 аналізувати та проводити оцінку ефективності

	та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН-29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН-33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН-34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібер-безпеки відповідно до цілей і завдань організації; РН-35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН-42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН-44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН-45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН-46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-10 виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН-11 виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; РН-13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на

	стандартизованих технологіях та протоколах передачі даних; РН-14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН-15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН-18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН-19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН-21 вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН-22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН-23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН-24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН-25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН-26 впроваджувати заходи та забезпечувати

	реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН-32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН-41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН-42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компо-ненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН-49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН-50 забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН-51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН-52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

Перелік тем семінарських / лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці “Рейтинг-план навчальної дисципліни”.

Змістовий модуль 1.
Організація управлінської діяльності

Тема 1. Еволюція управлінської думки.

Моделі менеджменту. Основні школі та підходи в управлінні. Організація як об’єкт управління. Аналіз організаційного середовища. SWOT, PEST аналіз. Проектування діяльності менеджера

Тема 2. Організаційні структури управління та принципи їх формування.

Види та особливості організаційних структур. Моделювання організаційної структури управління з урахуванням її місії та завдань.

Тема 3. Основи процесного підходу в управлінні.

Процесний підхід в управлінні підприємством. Етапи впровадження процесного підходу. Планування процесів в організації.

Тема 4. Комунікаційна політика організації.

Сутність, цілі, завдання, етапи розробки комунікаційної політики. Внутрішня та зовнішня комунікативна політика. Капітал публічності. Засоби. Аудит комунікативної політики організації.

Тема 5. Управлінські рішення і методи управління.

Сутність і класифікація методів управління, формулювання і діагностування проблеми, виявлення альтернативи її рішення і їх оцінка, оцінювання ефективності управлінських рішень.

Тема 6. Процес прийняття та реалізації управлінських рішень.

Природа процесу прийняття управлінських рішень та факторів впливу, алгоритми прийняття управлінських рішень, методи підготовки та реалізації управлінських рішень, збору, обробки та аналізу інформації з окремих проблем менеджменту, підходи реалізації різних груп методів управління в організації.

Змістовий модуль 2.
Інформаційне забезпечення управлінської діяльності

Тема 7. Інформація як частина управлінської діяльності.

Роль та місце інформації в управлінської діяльності. Види економічної інформації. Структура інформаційних потоків організації.

Тема 8. Нормативно-правове забезпечення суспільних інформаційних відносин.

Законодавче забезпечення формування інформаційних відносин. Формування правових кейсів та оформлення основних документів.

Тема 9. Інформаційне забезпечення як складова управлінської діяльності.

Визначення структури та формування інформаційного забезпечення. Визначення та задоволення інформаційних потреб, види інформаційних потоків, особливості прийняття управлінських рішень.

Тема 10. Розвиток електронного урядування: міжнародний досвід та відчизняна практика.

Національні інформаційні ресурси України. Тенденції розвитку корпоративних інформаційних систем. Проектування корпоративних інформаційних систем

Тема 11. Організаційно-виробничі структури та їхнє інформаційне забезпечення.

Види та особливості організаційно-виробничих структур. Канали інформаційного забезпечення.

Тема 12. Управлінські інформаційні системами — системи підтримки рішень.

Сучасні тенденції розвитку системи підтримки рішень. Постановка та реструктуризація інформаційних систем обліку в організації. Проектування інформаційних

систем обліку

Методи навчання та викладання

У процесі викладання навчальної дисципліни для активізації навчально-пізнавальної діяльності студентів передбачене застосування як активних, так і інтерактивних навчальних технологій, серед яких: лекції проблемного характеру, міні-лекції, робота в малих групах, семінари-дискусії, мозкові атаки, кейс-метод, презентації, банки візуального супроводу, індивідуально-дослідницька робота.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, семінарські та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, семінарських та лабораторних занять і оцінюється сумою набраних балів (максимальна сума — 60 балів; мінімальна сума, що дозволяє студенту складати іспит, — 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни — змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Поточний контроль включає оцінювання студентів під час:

лекцій – активна робота на парі (0,5 балів за кожне заняття) за умови активної участі студента в обговоренні дискусійних питань. Загальна кількість балів 6.

лабораторних та семінарських робіт – активна робота на парі (0,5 балів за кожне заняття) за умови участі студента в визначенні можливих методів виконання завдань; виконання практичних завдань (4 бали за кожне завдання) за умови правильного виконання отриманого завдання. Загальна кількість балів 22.

самостійної роботи – презентація результатів дослідження (4 балів за кожну презентацію) за умови обґрунтування отриманих результатів та надання пропозицій. Загальна кількість балів 8.

Колоквіум. Протягом семестру студенти пишуть два колоквіуми (по 12 балів кожен). Перший колоквіум включає теми з 1 по 6, другий теми з 7 по 11. Максимальна кількість балів за обидва колоквіуми – 24.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення іспиту. Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається з 10 тестів та 3 практичних завдань (ситуаційного, діагностичного, евристичного), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Екзаменаційний білет включає:

Тести: мах кількість балів 15

Ситуаційне завдання: мах кількість балів – 5.

Діагностичне завдання: мах кількість балів – 8.

Евристичне завдання: мах кількість балів 12.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами

підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру — 35 та мінімально можлива кількість балів, набраних на екзамені, — 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів — зараховано", "59 і менше балів — не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

Рейтинг план навчальної дисципліни
«Організація та інформаційне забезпечення управлінської діяльності»

Теми	Форми та види навчання		Форми оцінювання	Макс. бал
Аудиторна робота				
ТЕМА 1.	**Лекція**	Проблемна лекція: Вплив еволюції управлінської думки на організацію.	Активна робота на парі	**0,5**
	Семінарське заняття	Семінарське заняття: Основні школі та підходи управління	Активна робота на парі	**0,5**
ТЕМА 2.	**Лекція**	Лекція за питаннями: Види та особливості організаційних структур. Моделювання організаційної структури управління з урахуванням її місії та завдань.	Активна робота на парі	**0,5**
	Лабораторне заняття	Завдання з формування організаційної структури	Активна участь у виконанні практичних завдань	**0,5**
	Самостійна робота			
	Питання та завдання для самостійного опрацювання	Опрацювання лекційного матреіалу, підготовка презентації за проблемними питаннями теми1-2	Захист презентацій	**4**

ТЕМА 3	**Лекція**	Лекція за питаннями: Процесний підхід в управлінні підприємством. Етапи впровадження процесного підходу. Планування процесів в організації.	Активна робота на парі	**0,5**
	Лабораторне заняття	Завдання з планування процесів в організації.	Активна робота на парі	**0,5**
			Захист лабораторної роботи	**4**
ТЕМА 4.	**Лекція**	Лекція за темою: Комунікативна політика організації.	Активна робота на парі	**0,5**
	Лабораторне заняття	Тема завдання: Аудит комунікативної політики організації.	Активна робота на парі	**0,5**
	Самостійна робота			
	Питання та завдання для самостійного опрацювання	Опрацювання лекційного матеріалу	Перевірка ДЗ	
Аудиторна робота				
Тема 5	**Лекція**	Лекція за питаннями: Сутність і класифікація методів управління, формулювання і діагностування проблеми, виявлення альтернативи її рішення і їх оцінка, оцінювання ефективності управлінських рішень.	Активна робота на парі	**0,5**
	Лабораторне заняття	Оцінювання ефективності управлінських рішень.	Активна робота на парі	**0,5**
			Захист завдання	**4**
Тема 6.	**Лекція**	Лекція за темою: Процес прийняття та реалізації управлінських рішень.	Активна робота на парі	**0,5**
	Лабораторне заняття	Аналіз методів управління в організації	Активна робота на парі	**0,5**
		Підготовка до колоквіуму	Колоквіум	**12**
ТЕМА 7	**Лекція**	Лекція за питаннями: Роль та місце інформації в управлінській діяльності. Види економічної інформації. Структура інформаційних потоків організації.	Активна робота на парі	**0,5**
	Семінарське заняття	Структуризація управлінської інформації	Активна робота на парі	**0,5**
ТЕМА 8.	**Лекція**	Лекція за питаннями: Нормативно-правове забезпечення суспільних інформаційних відносин.	Активна робота на парі	**0,5**
	Лабораторне заняття	Оформлення основної документації	Активна робота на парі	**0,5**
			Захист завдання	**4**

ТЕМА 9.	**Лекція**	Лекція за питаннями: Інформаційне забезпечення як складова управлінської діяльності.	Активна робота на парі	**0,5**
	Лабораторне заняття	Структура інформаційних потоків організації	Активна робота на парі	**0,5**
ТЕМА 10.	**Лекція**	Лекція за питаннями: Розвиток електронного урядування: міжнародний досвід та відчиняння практика.	Активна робота на парі	**0,5**
	Лабораторне заняття	Завдання: Аналіз національних інформаційних ресурсів України	Активна робота на парі	**0,5**
			Захист завдання	**4**
ТЕМА 11	**Лекція**	Організаційно-виробничі структури та їхнє інформаційне забезпечення	Активна робота на парі	**0,5**
	Лабораторне заняття	Завдання: Аналіз та удосконалення каналів інформаційного забезпечення	Активна робота на парі	**0,5**
	Самостійна робота			
	Питання та завдання для самостійного опрацювання	Опрацювання лекційного матреіалу, підготовка презентації за обраними проблемними темами	Захист презентацій	**4**
Аудиторна робота				
ТЕМА 12	**Лекція**	Лекція за питаннями: Сучасні тенденції розвитку системи підтримки рішень. Постановка та реструктуризація інформаційних систем обліку в організації. Проектування інформаційних систем обліку	Активна робота на парі	**0,5**
	Лабораторне заняття	Аналіз інформаційних систем обліку	Активна робота на парі	**0,5**
		Підготовка до колоквіуму	Колоквіум	**12**
Іспит				**40**
	Загальна максимальна кількість балів по дисципліні			**100**

Рекомендована література

Основна література

1. Опорний конспект лекцій «Організація та інформаційне забезпечення управлінської діяльності» / уклад. В. В. Томах. Режим доступу. – https://pns.hneu.edu.ua/enrol/index.php?id=5213

Додаткова література:

2. Гончаренко О. М. Інформаційне забезпечення процесу прийняття управлінських рішень [Текст] / О. М. Гончаренко // Управління розвитком №16 (137) . – 2012 – С. 30-32

3. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія / І. В. Діордіца . — Запоріжжя : Гельветика, 2017. – 547 с.

4. Іваній Н. Інформаційні технології в професійній освіті / Н. Іваній // Освіта України . – 2004. – №20. – с.8

5. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. — На заміну ДСТУ ISO/IEC 27032:2015 ; Чинний від 2018-01-01. — Київ : УкрНДНЦ, 2018. — VI, 44 с.

6. Інформаційні технології: сучасний стан та перспективи [Текст] : монографія / за заг. ред. В.С. Пономаренка. – Х. : ДІСА ПЛЮС, 2018 – 461 с.

7. Кузнєцов Е. А. Методологія професіоналізації управлінської діяльності в Україні : монографія / Е. А. Кузнєцов. — Херсон : ОЛДІ-ПЛЮС, 2017. — 381 с.

8. Отенко В. І. Організаційне забезпечення формування професійних команд управлінського персоналу за допомогою соціоніки / В. І. Отенко, С. А. Доронін// Бизнес информ . – 2018. – №8. – 2018 – С. 217-224

9. Пономаренко В. С. Інформаційні технології в економіці: навч. посіб / В. С. Пономаренко, І. В. Журавльова. – Х. : ХДЕУ, 2000 – 137 с.

10. Проскуріна Н. М. Організація і методика документального забезпечення аудиту фінансової звітності в системі корпоративного управління : наук.-практ. посіб. / Н. М. Проскуріна, О. Ю. Рубітель ; за ред. проф. Н. М. Проскуриної. — Запоріжжя : ЗНУ, 2015. — 214 с.

11. Скляренко О.О. Інформаційні технології в системі інноваційного розвитку та трансферу технологій / О. О. Скляренко // Проблеми науки . – 2013. – №12. – 2013 – С. 17 - 20

12. Череп А. В. Інформаційне забезпечення в системі управління промисловим підприємством: монографія / А. В. Череп, О. М. Панченко, Л. А. Птіцина. — Запоріжжя : Запоріз. нац. ун-т, 2014. — 264 с.

13. Черноіванова Г. С. Організаційно-економічне забезпечення управління інноваціями та інноваційною працею : монографія / Г. С. Черноіванова. — Харків : [б. в.], 2018. — 284 с.

14. Ястремська О.М. Організаційне забезпечення якості трудової діяльності керівників промислових підприємств [Текст] : монографія / О. М. Ястремська, К. В. Яковенко, В. В. Томах // Харківський національний економічний університет. – Х. : ХНЕУ, 2009 – 327 с.

Інформаційні ресурси:

15. Організація та інформаційне забезпечення управлінської діяльності. – Режим доступу. – https://pns.hneu.edu.ua/enrol/index.php?id=5213

16. Асоціацію "IT Ukraine" [Електронний ресурс]. — Режим доступу. — https://itukraine.org.ua.

17. Державна служба статистки України / Офіційний веб-сайт : [Електронний ресурс]. — Режим доступу. — http://www.ukrstat.gov.ua.

18. Законодавство України / Офіційний сайт Верховної Ради України : [Електронний ресурс]. — Режим доступу. — http://zakon.rada.gov.ua.