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

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

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

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
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЄЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробники:
Євсеєв С. П., д.т.н., проф. кафедри КІТ,
Гаврилова А. А. ст. викл. кафедри КІТ,
Ткачов А.М., к.т.н., с.н.с., доц. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Організаційні заходи відіграють важливу роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей найчастіше обумовлені не тільки технічними аспектами, а й зловмисними діями, а також недбальством, недбалістю, халатністю користувачів або обслуговуючого персоналу, що ігнорує елементарні правила захисту. Закони та нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, що створюються в державі, відомствах, установах і організаціях. При розгляді питань захисту інформації така діяльність розглядається як організаційні методи забезпечення.

В інформаційних системах організаційні заходи виконують стрижневу роль в реалізації комплексної системи захисту інформації. Тільки за їх допомогою можливе об'єднання на правовій основі інженерно-технічних, програмно-апаратних, криптографічних та інших засобів захисту інформації в єдину комплексну систему.

Метою викладання дисципліни "Організаційне забезпечення захисту інформації" є формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами.

Результатами вивчення дисципліни є придбання навичок з формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**7**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Забезпечення інформаційної безпеки	Проектування систем захисту мереж наступного покоління
Організація та інформаційне забезпечення управлінської діяльності	Теорія ризиків
Комплексні системи захисту інформації	Переддипломна практика

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної

	діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; 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 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 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КФ 1. 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.	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 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–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 – 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 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; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації

Тема 1. *Завдання організаційного забезпечення захисту інформації*
Тема 2. *Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення*
Тема 3. *Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації*
Тема 4. *Служба безпеки об'єкта*
Тема 5. *Підбір, розстановка і робота з кадрами*

Змістовий модуль 2. Заходи з організації забезпечення захисту інформації на підприємствах

Тема 6. *Організація і забезпечення режиму таємності*
Тема 7. *Організація пропускного, внутрішньо об'єктового і протипожежного режиму*
Тема 8. *Захист інформації при аваріях та інших екстремальних ситуаціях*
Тема 9. *Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи

наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові проекти, майстер-класи.

Порядок оцінювання результатів навчання

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

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

2) модульний контроль, що проводиться у формі контрольної роботи 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;

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

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– застосовувати законодавчу та нормативно-правову базу України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– розробляти пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

– розробляти та втілювати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

– виявляти, ідентифікувати, аналізувати та реагувати на інциденти інформаційної і/або кібербезпеки;

– використовувати в професійній діяльності знання про різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

– аналізувати та мінімізувати ризики обробки інформації в інформаційно-телекомунікаційних системах.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекцій: за активну роботу на парі нараховуються бали, (1 бал за кожне заняття) за умови виконання студентом програми навчальної дисципліни. Загальна кількість балів складає 9.

Лабораторні заняття: за умови виконання лабораторної роботи нараховується 1 бал, за умови захисту лабораторної роботи нараховується 2 бали, максимальна кількість балів

становить 25, а мінімальна – 9.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Модульний контроль: проводиться у формі контрольної роботи 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. За кожну контрольну роботу може бути нараховано 10 балів. Загальна кількість балів складає 20.

Підсумковий контроль:

Формою підсумкового контролю є іспит. Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей. Кожен екзаменаційний білет складається із 20 тестів та 3 практичних завдань (ситуаційного, діагностичного та евристичного).

Екзаменаційний білет включає:

Тести: мах кількість балів – 14.

Ситуаційне завдання: мах кількість балів – 5.

Діагностичне завдання: мах кількість балів – 9.

Евристичне завдання: мах кількість балів – 12.

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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план 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

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Завдання організаційного забезпечення захисту інформації"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 *"Розробити організаційну структуру відділу захисту*	Виконання та захист лабораторної	1

		інформації в межах організаційної структури підприємства"	роботи № 1	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *"Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 *"Розробити посадові інструкції відділу захисту інформації підприємства з врахуванням міжпосадових зв'язків та зв'язків з відділами підприємств"*	Виконання та захист лабораторної роботи № 2	1 2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3 *"Визначення функцій системи захисту інформації підприємства"*	Виконання та захист лабораторної роботи № 3	1 2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Служба безпеки об'єкта"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота №4. *"Формування вимог щодо внутрішньо об'єктового режиму"*	Виконання та захист лабораторної роботи № 4	1 2

			Контрольна робота 1	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *"Підбір, розстановка і робота з кадрами"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. *"Розробка вимог щодо забезпечення охорони підприємства"*	Виконання та захист лабораторної роботи № 5	1 2
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Організація і забезпечення режиму таємності"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6. *"Проведення оцінки персоналу за допомогою модуля "HR"*	Виконання та захист лабораторної роботи № 6	1 2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Організація пропускного, внутрішньо об'єктового і протипожежного режиму"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №7. *" Підбір, набір та облік кадрів за допомогою модуля "HR".*	Виконання та захист лабораторної роботи № 7	1 2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Захист інформації при аваріях та інших екстремальних ситуаціях"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №8. "Контроль участі персоналу у заходах"	Виконання та захист лабораторної роботи №8	1 1
			Експрес-опитування	3

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Транспортний рівень"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №9. "Розроблення вимог щодо організації пропускного режиму на підприємстві"	Виконання та захист лабораторної роботи № 9	1 1
			Контрольна робота 2	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Екзамен				40

Рекомендована література

Основна

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

2. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.

3. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

4. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

Додаткова

5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

6. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.

7. Яремчук Ю. Є. Дослідженняя характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.

Інформаційні ресурси.

8. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" – К.: Департамент спеціальних телекомунікаційних систем та

захисту інформації Служби безпеки України. – 2000. [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_1023_75718671.pdf]

9. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв". – 2012 [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_5623_75714589.pdf].

10. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю / 27 березня 2019 р. за N 306/33277 [Електронний ресурс]. – Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].

11. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].

12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Організаційне забезпечення захисту інформації" https://pns.hneu.edu.ua/course/view.php?id=5382.