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

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**12 "Інформаційні технології"**
Спеціальність	**125 "Кібербезпека"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"Кібербезпека"**
Статус дисципліни	**обов'язкова**
Мова викладання, навчання та оцінювання	**українська**

Розробник(и):
к.т.н., доцент Підписано КЕП Ганна СОЛОДОВНИК

старший викладач Олена МЕРЛАК

Завідувач кафедри
кібербезпеки та
інформаційних технологій Ольга СТАРКОВА

Гарант програми Вячеслав ЛИМАРЕНКО

Харків
2023

ВСТУП

Навчальна дисципліна «Комплексні системи захисту інформації» призначена для здобувачів вищої освіти, що навчаються за освітньо-кваліфікаційним рівнем «бакалавр». Вивчення дисципліни передбачає формування у майбутніх спеціалістів умінь та компетенцій в сфері розробки та впровадження комплексних систем захисту інформації (КСЗІ).

В даний час набули широкого поширення засоби і методи несанкціонованого доступу і отримання інформації в кіберпросторі. Вони знаходять все більше застосування не тільки в діяльності державних правоохоронних органів розвинених держав, а й в діяльності хакерів і різного роду злочинних кіберугрупувань.

Необхідно пам'ятати, що природні канали витоку інформації утворюються спонтанно, в силу специфічних обставин, що склалися на об'єкті захисту. Що стосується штучних каналів витоку інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічних каналів витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводам і лініям зв'язку, високочастотне нав'язування і опромінення, установка в технічних засобах і приміщеннях відеокамер, мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах тощо.

Тому особливу роль і місце в діяльності по захисту інформації займають заходи щодо створення комплексного захисту, що враховують загрози національній і міжнародній безпеці і стабільності, в тому числі суспільству, особистості, державі, демократичних цінностей і суспільних інститутів, суверенітету, економіці, фінансовим установам, розвитку держави.

Метою навчальної дисципліни «Комплексні системи захисту інформації» є навчання студентів принципам побудови КСЗІ на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Завданнями навчальної дисципліни є вивчення основних засад та вивчення основних засад з наступних питань:

- проведення обстеження об'єктів інформаційної діяльності (ОІД) та інформаційно-телекомунікаційних систем (ІТС);
- розробка моделей загроз та порушника;
- впровадження засобів захисту інформації;

- виявлення втручання в роботу ІТС (кібератак, комп'ютерних шахрайств, каналів витоку інформації, несанкціонованого доступу до інформації);

- блокування каналів витоку інформації;

- здійснення оцінки захищеності інформації на ОІД та в ІТС.

- проведення аналізу ефективності КСЗІ.

Предметом навчальної дисципліни є методи, методики, інформаційно-комунікаційні технології, програмно-апаратне забезпечення комплексних систем захисту інформації, їх впровадження та супровід.

Об'єктом навчальної дисципліни є процес створення комплексної системи захисту інформації в інформаційно-комунікаційних системах від витоку інформації технічними каналами зв'язку, порядку проведення обстеження середовищ функціонування інформаційно телекомунікаційних систем.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
РН 1.	КЗ 1, КЗ 2, КЗ 3.
РН 2.	КЗ 1, КЗ 2, КЗ 4, КЗ 5.
РН 3.	КЗ 1, КЗ 2, КЗ 4, КЗ 5.
РН 4.	КЗ 1, КЗ 2, КЗ 4, КЗ 5.
РН 5.	КЗ 2, КЗ 4, КЗ 5.
РН 6.	КЗ 2.
РН 7.	КЗ 2, КЗ 4, КФ 1.
РН 8.	КЗ 2, КЗ 4, КФ 1.
РН 9.	КЗ 5, КФ 1, КФ 3, КФ 4, КФ 5, КФ 7, КФ 8, КФ 9, КФ 11, КФ 12.
РН 17.	КЗ 2, КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 8, КФ 11.
РН 24.	КЗ 1, КФ 4, КФ 5, КФ 9, КФ 11.
РН 27.	КЗ 1, КФ 4, КФ 5, КФ 6.
РН 29.	КФ 3, КФ 4, КФ 5, КФ 8, КФ 9, КФ 12.
РН 32.	КЗ 1, КФ 4, КФ 5, КФ 8, КФ 11.
РН 33.	КФ 1, КФ 4, КФ 8, КФ 9, КФ 12.
РН 34.	КФ 1, КФ 4, КФ 5, КФ 8, КФ 9, КФ 12.
РН 35.	КЗ 1, КФ 1, КФ 3, КФ 4, КФ 5, КФ 7, КФ 8, КФ 9, КФ 12.
РН 42.	КФ 4, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12.
РН 43.	КЗ 2, КФ 1, КФ 4, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12.
РН 44.	КФ 1, КФ 4, КФ 5, КФ 8, КФ 9, КФ 12.
РН 45.	КФ 4, КФ 5, КФ 8, КФ 9, КФ 12.
РН 46.	КФ 4, КФ 5, КФ 8, КФ 9, КФ 12.
РН 53.	КЗ 1, КЗ 4, КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 8, КФ 11, КФ 12.
РН 54.	КЗ 1, КЗ 2, КЗ 6, КЗ 7.

де КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

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.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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 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.

РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації

Тема 1. Головні принципи та етапи захисту від загроз. Нормативно-правове забезпечення захисту інформації

1.1. Принципи та етапи заходів щодо захисту від загроз.

Загальний аналіз проблем організовування захисту від будь-яких загроз. Етапи та види захисту від загроз для електронних інформаційних ресурсів інформаційно-телекомунікаційних систем.

1.2. Нормативно-правові акти України, які визначають необхідність створення КСЗІ в ІТС

Закон України «Про захист інформації в автоматизованих системах». «Положення про технічний захист інформації в Україні». «Концепція ТЗІ в Україні». «Положення про ТЗІ в Україні». Закон України «Про інформацію».

Закон України «Про доступ до публічної інформації». Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Закон України «Про захист персональних даних». Закон України «Про захист інформації в ІТС».

1.3. Організаційні засади забезпечення захисту інформації

Призначення створення комплексної системи захисту інформації. Захист інформації від витоку технічними каналами. Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів. Захист інформації від спеціального впливу на засоби обробки інформації. Зміст плану захисту інформації в системі. Порядок проведення державної експертизи системи захисту.

Тема 2. Сутність та задачі комплексної системи захисту інформації

2.1. Основні підходи до створення комплексної системи захисту інформації

Визначення основних понять. Особливості сучасного підприємства як системи. Історія розвитку засобів захисту інформації.

2.2. Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації. Критерії надійності захисту інформації. Значимість комплексного підходу до захисту інформації.

2.3. Основні стратегії захисту інформації

Значення стратегії захисту інформації. Стратегічні фактори, які можуть мати вирішальне значення в майбутньому. Особливості стратегічних рішень.

2.4. Розробка політики безпеки

Етапи побудови організаційної політики безпеки. Процеси, пов'язані з розробкою і реалізацією політики безпеки. Види політики безпеки: виборча і повноважна.

Тема 3. Здійснення захисту інформації на підприємстві

3.1. Визначення та аналіз загроз

Особливості проблем дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації. Виявлення та аналіз загроз захисту. Явища, фактори і умови, що створюють небезпеку порушення статусу інформації. Джерела дестабілізуючого впливу на інформацію. Методика виявлення способів впливу на інформацію.

3.2. Розробка плану захисту інформації

План ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту інформації з обмеженим доступом. Реалізація плану захисту інформації. Організація проведення обстеження об’єктів інформаційної діяльності. Організація розроблення системи захисту інформації.

3.3. Реалізація організаційних заходів захисту

Етапи розроблення і реалізації організаційних заходів. Задачі оперативного вирішення задач технічного захисту інформації. Організаційно - правові заходи щодо охорони державної таємниці.

3.4. Реалізація первинних технічних заходів захисту

Етапи реалізації первинних технічних заходів. Етапи реалізації основних технічних заходів захисту. Приймання, визначення повноти та якості робіт.

Тема 4. Захист інформації від витоку технічними каналами

4.1. Основні визначення та положення

Визначення основних понять. Нормативні документи, що визначають зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації. Основні та допоміжні технічні засоби.

4.2. Заходи щодо технічного захисту інформації (ТЗІ)

Етапи проведення організаційних заходів. Визначення каналів витоку інформації з обмеженим доступом та їх блокування завдяки підготовчим технічним заходам. Складові технічного заходу. Додаткові заходи захисту. Пристрої, що відносяться до засобів технічного захисту. Методики захисту інформації з обмеженим доступом в залежності від каналів витоку.

Тема 5. Захист інформації в комп'ютерній системі (КС) підприємства

5.1. Основні загрози інформації в КС підприємства

Визначення основних понять. Різновиди носіїв інформації. Проблеми захисту від несанкціонованого доступу. Класифікація загроз за результатом їх впливу на інформацію.

5.2. Основні напрями захисту

Визначення мети всіх заходів захисту інформації. Компоненти комплексної системи захисту інформації. Об’єкти комп’ютерної системи. Типові адміністративні та організаційні вимоги до комп’ютерної системи підприємства стосовно питань технічного захисту інформації.

5.3. Характеристики комп’ютерної системи

Мета створення комп’ютерної системи. Функціонально-логічна структура комп’ютерної системи. Ієрархія компонентів комп’ютерної системи як територіально розосередженої системи. Характеристика користувачів комп’ютерної системи. Категорії користувачів комп’ютерної системи. Порядок і механізми доступу до інформації з обмеженим доступом та компонентів комп’ютерної системи особами різних категорій користувачів. Характеристика оброблюваної в комп’ютерній системі інформації.

Змістовий модуль 2. Захист інформації на підприємстві

Тема 6. Різновиди та класифікація «Моделі порушника»

6.1. Структура «Моделі порушника»

Абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості. Цілі створення «Моделі порушника». Різновиди порушників. Класифікація порушників. Обмеження та припущення про характер дій можливих порушників.

6.2. Види представлень «Моделі порушника»

Відображення «Моделі порушника» у вигляді системи таблиць. Словесний опис «Моделі порушника». Математична модель впливу порушників. Сценарні моделі впливу кожного порушника на систему.

Тема 7. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах

7.1. Забезпечення захисту державних інформаційних ресурсів в мережах передачі даних

Впровадження комплексу технічних, криптографічних, організаційних та інших заходів і засобів захисту інформації, спрямованих на недопущення блокування та/або модифікації інформації, що захищається. Етапи отримання сертифікату відповідності або експертного висновку.

7.2. Контроль за забезпеченням захисту державних інформаційних ресурсів в ІТС

Порядок організації та здійснення контролю за забезпеченням захисту державних інформаційних ресурсів в ІТС. Ліквідація визначених порушень щодо забезпечення захисту державних інформаційних ресурсів. Відповідальність за порушення вимог із захисту державних інформаційних ресурсів.

Тема 8. Захист інформації веб-сторінки підприємства від несанкціонованого доступу

8.1. Вимоги із захисту WEB-сторінки підприємства

Склад КС, яка забезпечує функціонування WEB-сторінки підприємства. Вимоги щодо забезпечення цілісності загальнодоступної інформації WEB-сторінки та конфіденційності й цілісності технологічної інформації. Технології виявлення спроб несанкціонованого доступу до інформації WEB-сторінки та процесів, які з цією інформацією пов'язані.

8.2. Середовище користувачів та фізичне середовище ІТС підприємства

Категорії користувачів за рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування КС. Складові фізичного середовища, що призначене для розміщення, експлуатації, адміністрування WEB-сторінки установи.

8.3. Політика безпеки інформації WEB-сторінки підприємства

Складові узагальненої функціонально-логічної структури інформаційно-телекомунікаційної системи підприємства. Об'єкти комп'ютерної системи, на які повинна поширюватися політика безпеки інформації WEB-сторінки підприємства. Рівні послуг безпеки для забезпечення захисту інформації від загроз.

Тема 9. Підрозділ захисту інформації (ПЗІ) на підприємстві

9.1. Завдання та функції ПЗІ

Мета створення підрозділу захисту інформації. Правова основа для створення і діяльності ПЗІ. Завдання ПЗІ. Функції ПЗІ під час створення комплексної системи захисту інформації. Функції ПЗІ під час експлуатації комплексної системи захисту інформації.

9.2. Повноваження та відповідальність підрозділу захисту інформації

Права ПЗІ. Зобов'язання ПЗІ. Види відповідальності ПЗІ. Відповідальність співробітників ПЗІ в залежності від посади.

9.3. Штатний розклад та структура підрозділу захисту інформації

Структура ПЗІ, її склад і чисельність. Рівень освіти співробітників ПЗІ. Функціональні обов'язки, посади, фах співробітників ПЗІ.

Тема 10. Державний контроль за станом захисту інформації. Відповідальність за невиконання вимог захисту інформації

10.1. Організація проведення перевірок стану КСЗІ

Види перевірки стану КСЗІ. Порядок проведення перевірок стану КСЗІ. Кваліфікація порушень з КСЗІ.

10.2. Відповідальність за невиконання вимог захисту інформації

Знайомство з адміністративним та кримінальним кодексами щодо відповідальність за забезпечення захисту інформації.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2.

Таблиця 2

Перелік лабораторних занять

Назва завдання	Зміст
Тема 1, 2. Завдання 1. Дослідження структури об'єкту захисту	Дослідження об’єкта з метою визначення його складових, структурних підрозділів; визначення типу технологій передачі інформації на об’єкті, носіїв інформації, що використовуються для зберігання інформаційних ресурсів, та методи й засоби їх захисту
Тема 3, 4. Завдання 2. Ідентифікація небезпечних чинників на об'єктах захисту	Визначення переліку загроз інформаційним ресурсам та потокам; визначення ймовірності виникнення кожної загрози
Тема 5, 6. Завдання 3. Розробка «Моделі порушника»	Визначення груп порушників на об’єкті, що досліджується; обґрунтування мотивів порушень; розробка «Моделі порушника»
Тема 7, 8. Завдання 4. Розробка політики інформаційної безпеки	Визначення критичних напрямів захисту та основних небезпечних чинників; складання розділів політики інформаційної безпеки, які стосуються критичних напрямів
Тема 9, 10. Завдання 5. Аналіз наявних в приміщенні типів технічних засобів	Визначення типів технічних засобів приміщення; визначення можливих каналів витоку інформації; надання рекомендацій для підвищення рівня безпеки обраного для аналізу приміщення

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3.

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1-5. Завдання 1.	Вивчення лекційного матеріалу та нормативної бази України
Тема 6-10. Завдання 2.	Підготовка до лабораторних занять

Кількість годин лекційних, лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:
Словесні (лекція (Тема 1, 3, 4, 5, 7-10), проблемна лекція (Тема 2, 6)).
Наочні (демонстрація (Тема 1-10)).
Практичні (лабораторна робота (Тема 1-10)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних та лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів: для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формі диференційованого заліку або заліку.

Підсумкова оцінка за навчальною дисципліною визначається:

– для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю;

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

– поточний контроль: лабораторні навчальні завдання (100 балів);

– семестровий контроль: залік.

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. 144 с.

2. Хорошко В. О. Проєктування комплексних систем захисту інформації: підручник. Львів : Львівська політехніка, 2020. 320 с.

3. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації: навч. посібник. Львів : Новий світ-2000, 2021. 678 с.

4. Євсеєв, С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. Електрон. текстові дан. (12,3 МБ). Харків : ХНЕУ ім. С. Кузнеця, 2020. 221 с.: іл. Загол. з титул. екрану. Бібліогр.: с. 211-213. http://repository.hneu.edu.ua/handle/123456789/24508

5. Лабораторний практикум з системного аналізу та проєктування інформаційних систем [Електронний ресурс] : навчальний посібник / І.О. Ушакова, І.Б. Медведєва; Харківський національний економічний університет ім. С. Кузнеця. — Електрон. текстові дан. (307 МБ) — Харків : ХНЕУ ім. С. Кузнеця, 2022. — 250 с. : іл. — Загол. з титул. екрану. — Бібліогр.: с. 151-153. http://repository.hneu.edu.ua/handle/123456789/27815

6. «Про захист інформації в інформаційно-комунікаційних системах». Серія «Закони України». Київ : Паливода А.В., 2023. 12 с.

7. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

8. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

9. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

10. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

11. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

12. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

13. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Додаткова

14. Milov O. Self-organizing organizational structures of cybersecurity systems / O. Milov, V Aleksiyev. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. Vienna: Premier Publishing s.r.o., 2020. P. 65-78. http://repository.hneu.edu.ua/handle/123456789/24816

15. Martovytskyi V. Technology for monitoring the functioning state of distributed computer systems / V. Martovytskyi, Y. Koltun, D. Holubnychyi et al. //

Системи управління, навігації та зв’язку : зб. наук. пр. – 2022. – Вип. 1 (67). – С. 75-80. http://www.repository.hneu.edu.ua/handle/123456789/27369.

16. ISO/IEC 27001:2013. «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

17. ISO/IEC 27003. «Системи менеджменту інформаційної безпеки».

18. ISO/IEC 27006. «Вимоги до органів, що здійснюють аудит та сертифікацію систем менеджменту інформаційною безпекою».

Інформаційні ресурси

19. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Комплексні системи захисту інформації» https://pns.hneu.edu.ua/course/view.php?id=9755.