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

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та інформаційних технологій
Протокол № 11 від 03.02.2025 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

_____ Карина НЕМАШКАЛО

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни (РПНД)

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

Статус дисципліни	**обов'язкова**
Мова викладання, навчання та оцінювання	**українська**

Розробники
д.т.н., проф. Ольга СТАРКОВА

к.т.н. Олег ПОЧАНСЬКИЙ

Завідувач кафедри
кібербезпеки
та інформаційних технологій Ольга СТАРКОВА

Гарант програми Вячеслав ЛИМАРЕНКО

Харків
2025

ВСТУП

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. Під час розгляду 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. Крім того, курс включає розгляд питань, пов’язаних з аналізом можливості створення ефективного управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів за рахунок розгляду теоретичних основ менеджменту інцидентів безпеки, моделі PDCA та етапів ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044. Запропоновані до розгляду особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL, поняття групи реагування на інциденти інформаційної безпеки (CERT/CSIRT), інструментарій для ефективного функціонування груп реагування на інциденти інформаційної безпеки. Крім того, розглянуто можливі постановки задач аналізу інформаційних ризиків та управління ними при організації режиму інформаційної безпеки в компаніях. Розглянута міжнародна концепція забезпечення інформаційної безпеки, а також різні підходи і рекомендації щодо вирішення завдань аналізу ризиків та управління ними. Дан огляд основних стандартів в галузі захисту інформації та управління ризиками: ISO 17799, ISO 15408, BSI, NIST, MITRE. Наводяться інструментальні засоби для аналізу ризиків (COBRA, CRAMM, MethodWare, RiskWatch). Показаний взаємозв’язок завдань аналізу захищеності і виявлення вторгнень із завданням управління ризиками. Наведені технології оцінки ефективності забезпечення інформаційної безпеки в компаніях.

Мета навчальної дисципліни «Організаційне забезпечення захисту інформації» – формування теоретичних знань щодо організаційного забезпечення діяльності з захисту інформації, такої як: управління інцидентами інформаційної безпеки; аналіз і оцінка інформаційної безпеки об'єкта щодо його організаційного забезпечення; організації керування загрозами; реагування на інциденти; організації і забезпечення режиму таємності; підбору, розстановки і роботи з кадрами.

Завдання навчальної дисципліни – отримання знань, вмінь та навичок з організаційного забезпечення діяльності з захисту інформації, такої як: управління інцидентами інформаційної безпеки; аналіз і оцінка інформаційної безпеки об'єкта щодо його організаційного забезпечення; організації керування загрозами;

реагування на інциденти; організації і забезпечення режиму таємності; підбору, розстановки і роботи з кадрами.

Предметом вивчення дисципліни є процедури, методи та засоби організаційного забезпечення діяльності щодо інформаційної безпеки.

Об'єктом вивчення дисципліни є організаційне забезпечення захисту інформації.

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 3	ЗК 6, ЗК 7, СК 1.
РН 9	ЗК 6, ЗК 7, СК 1, СК 2.
РН 11	СК 2, СК 4.
РН 14	СК 4, СК 6, СК 10.
РН 15	СК 4, СК 6, СК 10.
РН 17	СК 4, СК 6, СК 10.
РН 20	ЗК 2, СК 4, СК 5, СК 6, СК 10.

де, ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

СК1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в

організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН20. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Управління інцидентами інформаційної безпеки.

Тема 1. Теоретичні основи менеджменту інформаційної безпеки. Менеджмент інциденту інформаційної безпеки

Базові терміни і поняття ІБ. Еволюція кіберзагроз. Критично важливі об’єкти інфраструктури України. Приклади кібератак. Аналіз способів розгортання шкідливого ПЗ. Проблеми кібербезпеки в інтернеті речей. Основні причини кіберпорушень. Базові поняття інцидент-менеджменту.

Короткий огляд проблеми управління ризиками. Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки. Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044.

Тема 2. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL. Група реагування на інциденти інформаційної безпеки

Міжнародний стандарт ITIL. Менеджмент інцидентів відповідно до стандарту ITIL. Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ. Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди підприємців. Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти.

Тема 3. Базові етапи створення груп CERT / CSIRT. Документаційний супровід функціонування груп реагування на інциденти інформаційної безпеки

Інструменти для моніторингу та реєстрації інциденту. Інструменти для обробки інциденту. Інструменти для розслідування інциденту. Інструменти для контролю каналів зв'язку та веб-ресурсів.

Інструментарій для ефективного функціонування груп реагування на інциденти ІБ. Документаційне забезпечення процесу управління інцидентами ІБ. Діяльність різних груп реагування на інциденти ІБ.

Тема 4. Управління ризиками та міжнародні стандарти. Технології аналізу ризиків.

Міжнародний стандарт ISO 31000. Етапи процесу управління ризиками. Рамкова програма з кібербезпеки. Основні функції рамкової програми. Рівні впровадження рамкової програми. Встановлення або вдосконалення програми кібербезпеки. Аудит інформаційної безпеки. Дослідження стану інформаційно-комунікаційної системи. Дослідження інформаційного середовища інформаційно-комунікаційної системи. Дослідження фізичного середовища інформаційно-комунікаційної системи. Дослідження середовища користувачів. Тестування на уразливість інформаційно-комунікаційної системи. Методи оцінки ризиків. Практичний ризик-менеджмент.

Тема 5. Політика системи менеджменту інформаційної безпеки. Інструментальні засоби аналізу ризиків

Система менеджменту інформаційної безпеки: орієнтовна послідовність дій при розробці, обов'язкові документи. Загальна політика інформаційної безпеки. Приклад структури (загальної і детальних) політик безпеки організації (для забезпечення мережевої безпеки). Приклад політики інформаційної безпеки. Приклади невдалих політик інформаційної безпеки. Фактори, що визначають ефективність політики безпеки. Політика інформаційної безпеки. Ідентифікація та оцінка активів. Аналіз джерел проблем. Ролі та обов’язки щодо інформаційної безпеки.

Змістовий модуль 2. Роль організаційного забезпечення при здійсненні захисту інформації. Організація доступності активів і робота з персоналом

Тема 6. Завдання організаційного забезпечення захисту інформації. Організаційні основи захисту інформації.

ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Забезпечення безпеки інформації на організаційному рівні. Організаційний захист. Основні організаційні заходи. Організаційні засоби захисту комп'ютерних інформаційних систем та мереж. Найкращі практики безпеки. Керівництво інформаційною безпекою. Групи принципів захисту інформації. Організаційно-технічні заходи щодо технічного захисту інформації. Групи реагування на інциденти з комп'ютерної безпеки. Збірка сценаріїв з організації захисту. Правові проблеми кібербезпеки. Етичні питання кібербезпеки. Кодекс ділової поведінки Cisco. Служба захисту інформації.

Тема 7. Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення. Організація керування загрозами.

Основні визначення. Рівні безпеки. Система забезпечення безпеки. Основні задачі забезпечення інформаційної безпеки. Джерела загроз інформаційній безпеці. Засоби впливу загроз на інформаційну безпеку. Класифікація загроз безпеки. Загальна схема управління безпекою бізнес-процесів. Методи запобігання та ліквідації загроз інформаційній безпеці. Захист від ланцюга кібервбивства. Загальні

загрози та вразливості користувачів, пристроїв, локальної мережі, приватної хмари, публічної хмари, фізичних об'єктів, застосунків.

Тема 8. Контроль доступу. Організація доступності.

Контроль фізичного доступу. Системи розмежування логічного доступу. Адміністративний контроль доступу. Ідентифікація та аутентифікація. Авторизація. Механізми розкриття порушень. Коригуючі, компенсуючі засоби контролю та засоби відновлення. Концепція п'яти дев'яток. Загрози доступності. Проєктування системи високої доступності. Використання багаторівневих систем захисту.

Тема 9. Реагування на інциденти.

Загальні поняття. Контроль доступу до мережі. Системи виявлення вторгнень. Системи запобігання вторгненням. Розширений аналіз загроз. Відновлення після катастроф. Безперервність бізнесу. Антикризове управління.

Тема 10. Підбір, розстановка і робота з кадрами. Організація і забезпечення режиму таємності.

Планування персоналу. Принципи планування чисельності і складу працівників. Залучення персоналу. Особливості відбору співробітників, які допускаються до роботи з конфіденційною інформацією. Організація секретного діловодства. Віднесення відомостей до комерційної таємниці. Захист службової інформації. Допуск громадян до державної таємниці.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2

Таблиця 2

Перелік лабораторних занять

Назва теми та / або завдання	Зміст
Тема 1. Лабораторна робота 1.	Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет. Нормативна база для забезпечення інформаційної безпеки держави. Потенційні загрози, засоби їх попередження та ліквідації
Тема 2. Лабораторна робота 2.	Моніторинг згадувань об’єктів (інцидентів з інформаційною безпекою) у мережі Інтернет
Тема 3. Лабораторна робота 3.	Організація діяльності відділу управління інформаційними ресурсами та захисту інформації
Тема 4. Лабораторна робота 4.	Процес управління ризиками інформаційної безпеки для забезпечення властивості живучості систем
Тема 5. Лабораторна робота 5.	Аналіз ринку аудиторських послуг в Україні
Тема 6. Лабораторна робота 6.	Робота з Центрами сертифікації безпеки
Тема 7. Лабораторна робота 7.	Аналіз інформації про технічне забезпечення організації, що знаходиться у відкритому доступі
Тема 8. Лабораторна робота 8.	Аналіз сертифікатів безпеки сайтів організацій
Тема 9. Лабораторна робота 9.	Моніторинг інформації, яка залишається у відкритому доступі, після ліквідації веб-ресурсів
Тема 10. Лабораторна робота 10.	Перевірка наявності службової інформації організації у відкритому доступі, після ліквідації веб-ресурсів

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1. Завдання 1	Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044.
Тема 2. Завдання 2.	Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти.
Тема 3. Завдання 3.	Діяльність різних груп реагування на інциденти ІБ.
Тема 4. Завдання 4.	Практичний ризик-менеджмент.
Тема 5. Завдання 5.	Політика інформаційної безпеки. Ідентифікація та оцінка активів. Аналіз джерел проблем. Ролі та обов'язки щодо інформаційної безпеки.
Тема 6. Завдання 6.	Кодекс ділової поведінки Cisco.
Тема 7. Завдання 7.	Загальні загрози та вразливості користувачів, пристроїв, локальної мережі, приватної хмари, публічної хмари, фізичних об'єктів, застосунків.
Тема 8. Завдання 8.	Проєктування системи високої доступності. Використання багаторівневих систем захисту.
Тема 9. Завдання 9.	Безперервність бізнесу. Антикризове управління.
Тема 10. Завдання 10.	Допуск громадян до державної таємниці.

Кількість годин лекційних та 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 (лекції 1-10), проблемна лекція (Тема 6).

Наочні (демонстрація (Тема 1-10)).

Практичні (лабораторні роботи (Теми 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, 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 екзамен (іспит): максимальна сума – 60 балів; мінімальна сума, що дозволяє здобувачу вищої освіти складати екзамен (іспит) – 35 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формах семестрового екзамену (іспиту). Складання семестрового екзамену (іспиту) здійснюється під час екзаменаційної сесії.

Максимальна сума балів, яку може отримати здобувач вищої освіти під час екзамену (іспиту) – 40 балів. Мінімальна сума, за якою екзамен (іспит) вважається складеним – 25 балів.

Підсумкова оцінка за навчальною дисципліною визначається для дисциплін з формою семестрового контролю екзамен (іспит) – сумуванням балів за поточний та підсумковий контроль.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

Поточний контроль: Лабораторні роботи (50 балів), письмові контрольні роботи (10 балів).

Семестровий контроль: Екзамен (40 балів).

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

Приклад фрагменту екзаменаційного білета

Харківський національний економічний університет імені Семена Кузнеця
Перший (бакалаврський) рівень вищої освіти
Спеціальність 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Кібербезпека»
Семестр IV
Навчальна дисципліна “Організаційне забезпечення захисту інформації”

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1

1.	До організаційно-правових засобів впливу загроз відносяться: A. перехоплення інформації в технічних каналах її витоку B. несанкціонований доступ до інформаційних ресурсів C. невиконання вимог законодавства та затримку прийняття необхідних нормативно правових положень в інформаційній сфері D. купівля недосконалих або застарілих інформаційних технологій та засобів інформатизації E. неправомірне обмеження доступу, до документів, в яких знаходиться важлива для громадян та організацій інформація
2.	Дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень, називається A. організаційно-технічний захід B. організаційно-правовий захід C. організаційно-економічний захід D. організаційно-соціальний захід

3.	Середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації – це A. інформаційний простір B. інформаційний ресурс C. інформаційна спільнота D. інформаційна інфраструктура
4.	Засоби впливу загроз поділяються на: A. інформаційні B. програмно-математичні C. фізичні D. економічні E. соціальні
5.	Співставте номери та назви Стандартів: 1 Інформаційні технології. Управління інформаційною безпекою 2 Інформаційні технології. Методи забезпечення безпеки. Системи керування інформаційною безпекою. Вимоги 3 Захист інформації. Технічний захист інформації. Порядок проведення робіт 4 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі A. ISO/IEC:17799 B. ISO/IEC 27001:2005 C. НД ТЗІ 3.7-003-05 D. НД ТЗІ 2.5-004-99 E. ДСТУ 3396.1-96
	Етап проведення аудиту інформаційної безпеки, пов'язаний з комплексним обстеженням ІТС, містить наступні складові: A. Обстеження обчислювальної системи B. Обстеження фізичного середовища C. Тестування на вразливості D. Обстеження інформаційного середовища E. Обстеження середовища користувачів F. Аналіз та систематизація отриманих результатів обстеження G. Ідентифікація отриманих вразливостей H. Оцінка рівня захищеності
7.	За поточним місцем розташування інформації розрізняють: A. Загрози доступу до інформації в оперативній пам'яті B. Загрози доступу до інформації на зовнішніх запам'ятовуючих пристроях C. Загрози доступу до інформації, що циркулює в лініях зв'язку D. Загрози доступу до інформації, яка відображається на терміналі або друкується на принтері E. Загрози, спрямовані на використання прямого стандартного шляху доступу до ресурсів F. Загрози, спрямовані на використання прихованого нестандартного шляху доступу до ресурсів G. Загрози, які можуть проявлятися незалежно від активності об'єкта H. Загрози, які можуть проявлятися тільки в процесі автоматизованої обробки даних
8.	Засоби впливу загроз поділяються на: A. інформаційні B. радіоелектронні C. організаційно-правові D. економічні E. соціальні
9.	Порушення цілісності, конфіденційності та доступності інформації полягає у: A. навмисний зміні інформації B. розкритті інформації тому, хто не має повноважень стосовно доступу до неї C. блокуванні доступу до деякого ресурсу D. виборі користувачем незахищених паролів E. використанні користувачем незахищених підключень

10.	Яка із функцій інформаційного простору сприяє створенню особливого середовища транскордонної, інтерактивної і мобільної комунікації різних суб'єктів економічної діяльності, у рамках якої вони здійснюють інформаційний обмін A. інтегруюча B. комунікативна C. актуалізуюча D. геополітична E. соціальна
...	...
71.	Законодавство України про державну таємницю включає наступні документи: A. Конституція України B. Закон України “Про державну таємницю” C. Закон України “Про персональні дані” D. Закон України “Про захист інформації” E. Всі перелічені
72.	Стандарт ISO 31000 рекомендує організаціям розвивати, впроваджувати та постійно вдосконалювати систему ризик-менеджменту, що забезпечує інтеграцію процесу управління ризиками з: A. стратегією та плануванням B. керівництвом C. цінностями та культурою D. політикою організації E. процесами звітності F. суспільством і державою G. всі варіанти правильні H. не має жодного правильного варіанту
73.	Згідно принципів управління ризиком (відповідно до ISO 31000) ризик-менеджмент: A. сприяє досягненню цілей та покращенню показників діяльності B. є складовою всіх організаційних процесів C. заснований на недоступній інформації D. є частиною прийняття рішення E. не враховує людські та культурні фактори F. чітко пояснює невизначеність G. все перелічене H. нічого з переліченого
74.	Етапи управління ризиками A. Встановлення контексту B. Комунікації та консультації C. Оцінка ризику D. Моніторинг та аналіз E. Обробка ризику F. Доручення й зобов’язання G. Впровадження системи та процесів ризик-менеджменту H. Проект концепції ризик-менеджменту
75.	Як називається тип заходів для відновлення ІТ-компанії після аварії, за якого застосовуються засоби контролю, що запобігають катастрофі A. запобіжні заходи B. розпізнавальні заходи C. коригувальні заходи D. нейтралізуючі заходи E. аналітичні заходи
76.	??? - це певні розгорнуті реальні бар'єри, які мають запобігти прямому контакту з інформаційними системами. A. Розмежування логічного доступу B. Адміністративний контроль доступу C. Контроль фізичного доступу

77.	Якого центру сертифікації безпеки не існує A. GeoTrust B. GoGetSSL C. RapidSSL D. Sectigo E. Email & Document Signing
78.	Яким документом унормовано державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики? A. Конституцією України B. Законом України “Про державну таємницю” C. Законом України “Про персональні дані” D. Законом України “Про захист інформації”
79.	Яка із складових етапу комплексного обстеження ІТС містить наступні роботи: 1) Збір відомостей про наявність у приміщеннях, де функціонує ІТС, елементів комунікацій, систем життєзабезпечення та зв'язку, що мають вихід за межі контрольованої території. 2) Збір відомостей про наявність системи заземлення обладнання ІТС та її технічні характеристики. 3) Збір відомостей про умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації. 4) Аналіз отриманої інформації. A. Обстеження фізичного середовища ІТС B. Тестування на вразливості ІТС C. Обстеження інформаційного середовища ІТС D. Обстеження обчислювальної системи ІТС E. Обстеження середовища користувачів
80.	Етап проведення аудиту інформаційної безпеки, пов'язаний з комплексним обстеженням ІТС, містить наступні складові: A. Оцінка рівня захищеності B. Обстеження обчислювальної системи C. Ідентифікація отриманих вразливостей D. Аналіз та систематизація отриманих результатів обстеження E. Обстеження середовища користувачів F. Обстеження фізичного середовища G. Обстеження інформаційного середовища H. Тестування на вразливості

Затверджено на засіданні кафедри КІТ протокол № _____від «_____»_20___р.

Екзаменатор д.т.н., проф. Старкова О.В.

Зав. кафедрою д.т.н., проф. Старкова О.В.

Критерії оцінювання

Перевірка теоретичних знань проводиться у вигляді тестування на платформі ПНС. Екзаменаційний білет складається з 80-ти тестових питань, правильна відповідь на кожне з яких оцінюється в 1 бал. У підсумкову оцінку кожна правильна відповідь входить з коефіцієнтом 0,5. Максимально можлива кількість балів за екзамен – 40.

Питання тесту охоплюють матеріали лекційного курсу, включно з завданнями на самостійну роботу, а також питання, що обговорювалися під час виконання лабораторних робіт. В тест включені:

Кількість питань в тесті	Назва теми
7	Теоретичні основи менеджменту інформаційної безпеки. Менеджмент інциденту інформаційної безпеки
4	Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL. Група реагування на інциденти інформаційної безпеки

8	Базові етапи створення груп CERT / CSIRT. Документаційний супровід функціонування груп реагування на інциденти інформаційної безпеки
14	Управління ризиками та міжнародні стандарти. Технології аналізу ризиків
8	Політика системи менеджменту інформаційної безпеки. Інструментальні засоби аналізу ризиків
4	Завдання організаційного забезпечення захисту інформації. Організаційні основи захисту інформації
7	Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення. Організація керування загрозами
14	Контроль доступу. Організація доступності
8	Реагування на інциденти
6	Підбір, розстановка і робота з кадрами. Організація і забезпечення режиму таємності

Питання за темами в тесті розміщені в довільному порядку.

Тест містить завдання трьох типів:

1) питання з можливістю вибору однієї або кількох правильних відповідей;

2) питання, яке передбачає розміщення у реченні пропущених слів (слова обираються із запропонованих варіантів);

3) питання, яке передбачає співставлення правильних тверджень (обираються із запропонованих варіантів).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Інформаційна безпека / за ред. Ю.Я.Бобала, І.В. Горбатого. Львів : Львівська політехніка, 2019. – 580 с.
2. Хорошко В.О. Проектування комплексних систем захисту інформації. Львів : Львівська політехніка, 2020. – 320 с.
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Львів: Магнолія, 2018. – 320 с.
4. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2021. – 272 с.
5. Остапов С. Е. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ-2000, 2021. – 679 с.
6. 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. http://www.repository.hneu.edu.ua/handle/123456789/24508
7. Солодовник Г. В. Методи та системи штучного інтелекту : навчальний посібник. – Харків: ТОВ «ДІСА ПЛЮС», 2021. -177 с. http://repository.hneu.edu.ua/handle/123456789/34052

Додаткова

8. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту

системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

9. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

10. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

11. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Київ : Департамент спеціальних телекомунікаційних систем та 11 захисту інформації Служби безпеки України. 2000. [Електронний ресурс]. Режим доступу : http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

12. ДСТУ 3396.1-96. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Режим доступу : https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf

13. Голубничий Д. Ю. Функціональна модель управління системою інформаційної безпеки / Д. Ю. Голубничий, В. Ф. Третяк, Д. М. Запара та ін. // Theoretical and practical aspects of development of legal knowledge, national security and physical education of citizens: Collective Scientific Monograph (1st edition). Tomkins R. (ed.). - Dallas, USA: Primedia eLaunch LLC, 2022. – С. 68–79. http://repository.hneu.edu.ua/handle/123456789/28326

14. Сучасні інформаційні технології та системи [Електронний ресурс] : монографія / Н. Г. Аксак, Л. Е. Гризун, О. В. Щербаков [та ін.] ; за заг. ред. Пономаренка В. С. — Електрон. текстові дан. (22,9 МБ). — Харків : ХНЕУ ім. С. Кузнеця, 2022. — 270 с. http://repository.hneu.edu.ua/handle/123456789/29233

Інформаційні ресурси

13. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Організаційне забезпечення захисту інформації" https://pns.hneu.edu.ua/course/view.php?id=11917