Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


_____ Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

«_29_» ____серпня____2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека»
(код і найменування спеціальності)

Освітня програма: «Безпека інформаційних і комунікаційних систем»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): __Андрій Карпенко, ст. викладач, д-р філософії_ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____
__комп’ютерних систем, мереж і кібербезпеки_____
(назва кафедри)

Протокол № 1 від « 29» серпня 2025 р.

Завідувач кафедри д.т.н., професор _____ _Вячеслав Харченко___
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК_____
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Карпенко Андрій Сергійович

Посада: старший викладач

Науковий ступінь: Ph.D.

Вчене звання: відсутнє

Перелік дисциплін, які викладає:
захист інформації в комп'ютерних мережах, теоретичні основи криптології, управління інформаційною безпекою, теорія та технології розробки безпечних розподілених систем.

Напрями наукових досліджень:
хмарні технології, кібербезпека, тестування програмного забезпечення.

Контактна інформація:
a.karpenko@csn.khai.edu, +380507095250

2. Опис навчальної дисципліни

Форма здобуття освіти	*денна*
Семестр	8-й
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 4 кредитів ЄКТС / 135 годин (64 аудиторних, з яких: лекції – 32, лабораторні – 32; СРЗ – 71);
Види навчальної діяльності	Лекції, лабораторні заняття, розрахункова робота, самостійна робота.
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – залік.
Пререквізити	Вища математика, дискретна математика, фізика, моделі та структури даних

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – діяльності на основі застосування системи теоретичних знань і практичних навичок, з: формування комплексу засобів (правил, процедур, тощо) щодо управління інформаційною безпекою; застосування комплексного підходу з забезпечення інформаційної безпеки в різних сферах діяльності (критичні системи та додатки).

Завдання – знати структуру нормативних актів та стандартів в сфері управління інформаційної безпекою; систему термінів понять; організовувати основні процеси реалізації систем ІБ, а саме, планування, ризик-аналізу, вибору контрзаходів, тощо; вміти використовувати сучасні інформаційні технології при оцінювання ризиків критичної інфраструктури; визначати шляхи зниження ризиків, практично застосовувати методи забезпечення безпеки.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(ЗК1) здатність застосовувати знання у практичних ситуаціях.

(ЗК2) знання та розуміння предметної області та розуміння професії.

(ЗК3) здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

(ЗК4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

(ЗК5) здатність до пошуку, оброблення та аналізу інформації.

(ЗК7) 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.***Спеціальні компетентності***

Після закінчення цієї програми здобувач освіти буде здатен:

(КФ1) 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.

(КФ2) здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

(КФ3) здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

(КФ4) здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

(КФ5) здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

(КФ6) здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

(КФ7) здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

(КФ8) здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

(КФ9) здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

(КФ10) здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

(КФ11) здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

(КФ12) здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

(ПРН1) застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

(ПРН2) організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

(ПРН3) використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

(ПРН4) 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.

(ПРН5) адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

(ПРН7) діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

(ПРН8) готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

(ПРН9) впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

(ПРН10) виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

(ПРН11) виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

(ПРН12) розробляти моделі загроз та порушника.

(ПРН14) вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

(ПРН21) 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.

(ПРН22) вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

(ПРН24) вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

(ПРН25) 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.

(ПРН26) впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

(ПРН30) здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

(ПРН32) вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

(ПРН33) вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

(ПРН34) приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

(ПРН41) забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

(ПРН42) впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

(ПРН43) застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

(ПРН44) 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.

(ПРН45) застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

(ПРН46) здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

(ПРН49) забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

(ПРН52) використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Теоретичні основи та міжнародний досвід управління інформаційною безпекою

Тема 1. Вступ до навчальної дисципліни. Основи управління інформаційною безпекою

Анотація: Розглядаються цілі, завдання, передумови та напрямки організаційної та управлінської роботи у сфері інформаційної безпеки. Вивчаються поняття ризику та загрози, їх класифікація. Аналізуються системи управління інформаційною безпекою (СУІБ) та модель PDCA. Розглядається діяльність міжнародних організацій в сфері інформаційної безпеки (ISO, ITU, IETF).

Тема лекції 1: Предмет, мета вивчення і задачі дисципліни. Загальні відомості про інформаційну безпеку. Ризики та їх класифікація. Способи порушення інформаційної безпеки.

Тема лекції 2: Система управління інформаційною безпекою (СУІБ). Модель PDCA. Діяльність міжнародних організацій в сфері інформаційної безпеки: ISO, ITU, IETF.

Лабораторна робота 1: Аналіз ризиків інформаційної безпеки підприємства. Ідентифікація та класифікація загроз.

Самостійна робота здобувачів: Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки. Сучасні технології захисту інформації. Структура та функції СУІБ. Опрацювання матеріалу лекцій, підготовка до модульного контролю.

Тема 2. Стандартизація в сфері менеджменту інформаційної безпеки

Анотація: Вивчаються основні стандарти в галузі інформаційної безпеки: серія ISO/IEC 27000, BS 7799, стандарти NIST. Розглядається робота спеціалізованих міжнародних організацій та об'єднань: ISACA, ISC², SANS Institute, CERT/CC. Аналізуються методології COBIT, ITIL/ITSM.

Тема лекції 3: Стандартизація в сфері менеджменту інформаційної безпеки. Серія стандартів ISO/IEC 27000. Британський стандарт BS 7799. Стандарти NIST.

Тема лекції 4: Роботи спеціалізованих міжнародних організацій та об'єднань в галузі інформаційної безпеки. ISACA, ISC², SANS Institute. Методології COBIT та ITIL/ITSM.

Самостійна робота здобувачів: Порівняльний аналіз міжнародних стандартів інформаційної безпеки. Сертифікація фахівців з інформаційної безпеки (CISSP, CISM, CISA). Опрацювання матеріалу лекцій.

Тема 3. Управління інформаційною безпекою на рівні постачальників та державному рівні

Анотація: Розглядаються підходи великих постачальників інформаційних систем (Microsoft, IBM, Oracle, Cisco) до управління інформаційною безпекою. Вивчається організаційне забезпечення інформаційної безпеки на державному рівні на прикладі США: NIST, NSA, CISA, законодавча база.

Тема лекції 5: Управління інформаційною безпекою на рівні великих постачальників інформаційних систем. Microsoft Security Development Lifecycle. Підходи IBM, Oracle, Cisco.

Тема лекції 6: Організаційне забезпечення інформаційної безпеки на державному рівні: практика США. NIST Cybersecurity Framework. Роль NSA та CISA.

Лабораторна робота 2: Аналіз та застосування NIST Cybersecurity Framework для оцінки стану інформаційної безпеки організації.

Самостійна робота здобувачів: Порівняння підходів різних постачальників до забезпечення безпеки програмних продуктів. Законодавство США в сфері інформаційної безпеки.

Тема 4. Забезпечення інформаційної безпеки на державному рівні: практика України

Анотація: Вивчається нормативно-правова база України в сфері інформаційної безпеки. Розглядаються криптографічні та технічні методи захисту інформації відповідно до вимог ДСТСЗІ СБУ та Держспецзв'язку. Аналізуються НД ТЗІ та КСЗІ.

Тема лекції 7: Забезпечення інформаційної безпеки на державному рівні: практика України. Нормативно-правова база. Закон України "Про захист інформації в ІТС". Роль ДСТСЗІ СБУ та Держспецзв'язку.

Тема лекції 8: Криптографічні методи захисту інформації в Україні. Вимоги до КСЗІ. Сертифікація засобів криптографічного захисту. НД ТЗІ.

Лабораторна робота 3: Аналіз нормативних документів системи технічного захисту інформації України. Розробка технічного завдання на КСЗІ.

Самостійна робота здобувачів: Структура системи технічного захисту інформації в Україні. Порядок створення та атестації КСЗІ. Опрацювання матеріалу лекцій.

Модульний контроль 1

Змістовний модуль 1. Практичні аспекти управління інформаційною безпекою на рівні підприємства

Тема 5. Технічні методи захисту та політика безпеки підприємства

Анотація: Розглядаються технічні методи захисту інформації: мережевий захист, криптографія, контроль доступу. Вивчаються основні напрямки та структура політики безпеки підприємства. Аналізуються вимоги до формування політики інформаційної безпеки відповідно до ISO/IEC 27001.

Тема лекції 9: Технічні методи захисту інформації на державному та корпоративному рівні. Мережевий захист, міжмережеві екрани, системи виявлення вторгнень.

Тема лекції 10: Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки. Формування політики ІБ за ISO/IEC 27001.

Лабораторна робота 4: Розробка політики інформаційної безпеки підприємства відповідно до вимог ISO/IEC 27001.

Самостійна робота здобувачів: Технічні засоби захисту інформації. Структура та компоненти політики безпеки. Процес розробки та впровадження політики ІБ.

Тема 6. Деталізована політика безпеки та робота з персоналом

Анотація: Вивчається зміст деталізованої політики безпеки: політика управління доступом, політика використання мережі, політика резервного копіювання. Розглядаються організаційна структура департаменту інформаційної безпеки та принципи роботи з персоналом.

Тема лекції 11: Зміст деталізованої політики безпеки. Політика управління доступом. Політика використання мережі та електронної пошти. Політика резервного копіювання.

Тема лекції 12: Департамент інформаційної безпеки: структура, функції, взаємодія з іншими підрозділами. Робота з персоналом: навчання, підвищення обізнаності, відповідальність.

Лабораторна робота 5: Розробка деталізованих політик безпеки: політика управління паролями, політика використання мобільних пристроїв.

Самостійна робота здобувачів: Типові деталізовані політики безпеки. Організація служби інформаційної безпеки на підприємстві. Програми підвищення обізнаності персоналу.

Тема 7. Реагування на інциденти та аудит інформаційної безпеки

Анотація: Розглядається організація процесу реагування на інциденти інформаційної безпеки: виявлення, аналіз, локалізація, ліквідація наслідків. Вивчаються методи та процедури аудиту стану інформаційної безпеки на підприємстві.

Тема лекції 13: Організація реагування на надзвичайні ситуації (інциденти). Класифікація інцидентів. Процедури виявлення, аналізу та реагування. CERT/CSIRT.

Тема лекції 14: Аудит стану інформаційної безпеки на підприємстві. Види аудиту. Методологія проведення аудиту. Звітність та рекомендації.

Лабораторна робота 6: Розробка плану реагування на інциденти інформаційної безпеки. Моделювання реагування на типові інциденти.

Самостійна робота здобувачів: Стандарти управління інцидентами (ISO/IEC 27035). Методи проведення аудиту ІБ. Інструменти автоматизації аудиту.

Тема 8. Надання послуг та міжнародний стандарт ISO/IEC 27001

Анотація: Вивчаються види послуг у сфері інформаційної безпеки: консалтинг, пентестування, SOC-послуги, страхування кіберризиків. Детально розглядається міжнародний стандарт ISO/IEC 27001: структура, вимоги, перелік захисних заходів (Annex A), процес сертифікації.

Тема лекції 15: Надання послуг у сфері інформаційної безпеки. Консалтинг, аутсорсинг безпеки, пентестування. Страхування кіберризиків.

Тема лекції 16: Міжнародний стандарт ISO/IEC 27001: структура, вимоги, перелік захисних заходів та їх цілей. Процес сертифікації СУІБ.

Лабораторна робота 7: Аналіз вимог ISO/IEC 27001. Розробка плану впровадження СУІБ на підприємстві.

Лабораторна робота 8: Практична реалізація захисних заходів ISO/IEC 27001 Annex A. Підготовка документації для сертифікації.

Самостійна робота здобувачів: Ринок послуг інформаційної безпеки. Вибір постачальника послуг ІБ. Детальне вивчення всіх доменів ISO/IEC 27001.

Модульний контроль 2

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

7. Методи контролю

Поточний контроль: опитування на лекційних та лабораторних заняттях з основних понять управління інформаційною безпекою, систем управління інформаційною безпекою (СУІБ) та міжнародних стандартів; аналіз та порівняння підходів до управління ІБ на різних рівнях (міжнародному, державному, корпоративному); виконання письмових контрольних робіт з окремих розділів курсу (ризики та загрози ІБ, міжнародні стандарти, державне регулювання, політика безпеки, реагування на інциденти, аудит ІБ, ISO/IEC 27001); програмований контроль (тестування, онлайн-тести) з теоретичних основ та практичних аспектів управління інформаційною безпекою; оцінювання виконання індивідуальних лабораторних робіт з аналізу ризиків, застосування NIST Cybersecurity Framework, розробки політик безпеки, планування реагування на інциденти, аналізу вимог ISO/IEC 27001; перевірка звітів з лабораторних робіт та їх захист; оцінювання виконання індивідуальних завдань з аналізу нормативної бази та розробки документації СУІБ.

Модульний контроль: складання модульного контролю з змістового модуля 1 "Теоретичні основи та міжнародний досвід управління інформаційною безпекою" та змістового модуля 2 "Практичні аспекти управління інформаційною безпекою на рівні підприємства"; перевірка знань з основ СУІБ, моделі PDCA, міжнародних стандартів серії ISO/IEC 27000, діяльності міжнародних організацій, державного регулювання ІБ в Україні та США, структури та змісту політики безпеки, управління інцидентами, аудиту ІБ; оцінювання практичних навичок розробки політик безпеки, аналізу ризиків, планування впровадження СУІБ та підготовки до сертифікації.

Підсумковий контроль: залік, що включає теоретичні питання з усіх розділів курсу та практичні завдання з аналізу ризиків інформаційної безпеки, розробки політики безпеки підприємства, планування реагування на інциденти, проведення аудиту ІБ, застосування вимог ISO/IEC 27001 для побудови та сертифікації системи управління інформаційною безпекою.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1 Змістовний модуль 1			
Робота на лекціях	0...1	8	0...8
Лабораторні заняття	0...6	4	0...24
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Робота на лекціях	0...1	8	0...8
Лабораторні заняття	0...6	4	0…24
Модульний контроль	0…18	1	0…18
Усього за семестр			**0…100**

Семестровий контроль (залік) проводиться у разі відмови здобувача освіти від балів підсумкового контролю. Під час складання семестрового заліку здобувач освіти має можливість отримати максимум 100 балів.

Білет для заліку складається з двох теоретичних і одного практичного запитання. За теоретичні запитання студент отримує до 60 балів (до 30 балів за кожне) , за практичне – до 40 балів. Під час складання семестрового заліку здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав два модульні контрольні роботи. Знає основні визначення та термінологію в галузі управління інформаційною безпекою. Розуміє поняття ризику та загрози, їх класифікацію. Знає структуру та функції системи управління інформаційною безпекою (СУІБ). Пояснює модель PDCA та її застосування в управлінні ІБ. Описує діяльність основних міжнародних організацій в сфері ІБ (ISO, ITU, IETF). Знає основні стандарти серії ISO/IEC 27000. Розуміє структуру державного регулювання ІБ в Україні та США. Описує базові принципи формування політики безпеки підприємства. Знає поняття інциденту ІБ та

основні етапи реагування. Описує базові принципи аудиту інформаційної безпеки. Виконує лабораторні роботи з аналізу ризиків, розробки політик безпеки та аналізу вимог стандартів. Використовує стандартні методи та інструменти для розв'язання базових задач управління ІБ.

Добре (75-89) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав два модульні контрольні роботи. Додатково до вимог на оцінку "задовільно": Проводить порівняльний аналіз міжнародних стандартів ІБ (ISO/IEC 27001, NIST, COBIT), порівнює їх ефективність та область застосування. Самостійно аналізує ризики інформаційної безпеки та розробляє заходи з їх мінімізації. Застосовує NIST Cybersecurity Framework для оцінки стану ІБ організації. Знає структуру та особливості нормативно-правової бази України в сфері ІБ (НД ТЗІ, вимоги до КСЗІ). Аналізує різні типи політик безпеки та обґрунтовує їх застосування для конкретних організацій. Самостійно розробляє деталізовані політики безпеки (управління доступом, резервне копіювання, використання мережі). Розуміє організаційну структуру департаменту ІБ та принципи роботи з персоналом. Знає процедури реагування на інциденти та класифікацію інцидентів. Проводить базовий аудит ІБ та формулює рекомендації. Порівнює різні підходи до управління ІБ та обґрунтовує вибір оптимальних рішень для конкретних сценаріїв.

Відмінно (90-100) – здобувач має глибокі знання, навички та вміння для досягнення результатів навчання за програмою на високому рівні. Написав два модульні контрольні роботи на відмінно. Додатково до вимог на оцінку "добре": Вільно оперує термінологією управління інформаційною безпекою та міжнародних стандартів. Самостійно проектує систему управління інформаційною безпекою відповідно до вимог ISO/IEC 27001. Обґрунтовує вибір захисних заходів (Annex A) для конкретних організацій з урахуванням їх специфіки та ризиків. Розробляє комплексну політику інформаційної безпеки підприємства з усіма деталізованими політиками. Самостійно планує та проводить повний цикл управління інцидентами ІБ. Проектує процедури аудиту ІБ та розробляє програму аудиту для організації. Аналізує ринок послуг ІБ та обґрунтовує вибір постачальників. Розробляє план впровадження СУІБ та підготовки до сертифікації за ISO/IEC 27001. Демонструє творчий підхід до розв'язання нестандартних задач управління інформаційною безпекою, пропонує інноваційні рішення для побудови ефективної СУІБ з урахуванням сучасних загроз та тенденцій розвитку інформаційних технологій.

9. Політика навчального курсу

Відвідування занять. Обов'язкове відвідування лекційних та лабораторних занять з навчальної дисципліни "Управління інформаційною безпекою" через їх інтерактивний характер та необхідність практичного

освоєння методів аналізу ризиків інформаційної безпеки, розробки політик безпеки, планування реагування на інциденти, проведення аудиту ІБ та застосування вимог міжнародних стандартів для побудови системи управління інформаційною безпекою. Здобувачі освіти, які не можуть регулярно відвідувати заняття, зобов'язані узгодити з викладачем протягом тижня графік відпрацювання пропущених занять. Пропущені заняття необхідно відпрацювати під час найближчої консультації протягом тижня з моменту пропуску, як правило, у формі усного опитування за попередньо визначеними питаннями з відповідних тем курсу. У деяких випадках допускається відпрацювання пропущених лабораторних занять у формі виконання письмових завдань з аналізу ризиків, розробки елементів політики безпеки, аналізу вимог стандартів або підготовки документації СУІБ. Пропуск модульних контрольних робіт без поважної причини не допускається.

Дотримання вимог академічної доброчесності Здобувачі освіти зобов'язані дотримуватися загальних морально-етичних норм, а також вимог академічної доброчесності, викладених у "Положенні про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут»" (https://khal.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Роботи здобувачів освіти (звіти з лабораторних робіт, розрахункова робота, модульні контрольні роботи) повинні бути оригінальними. Прикладами порушення академічної доброчесності є відсутність посилань на джерела, вигадування джерел, плагіат, перешкоджання роботі інших здобувачів освіти. Виявлення ознак порушення академічної доброчесності в письмових роботах (звітах з лабораторних робіт, розрахунковій роботі, модульних контрольних роботах) призводить до оцінки "незадовільно" незалежно від масштабу плагіату або обману. Особлива увага приділяється оригінальності програмного коду, реалізованого під час лабораторних робіт з дослідження криптографічних алгоритмів та стеганографічних методів. Використання готових рішень без посилань на джерела та без власного аналізу та модифікації вважається порушенням академічної доброчесності.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khal.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор»: [Ел. ресурс]. https://mentor.khai.edu/course/view.php?id=1611.

11. Рекомендована література

Базова

1. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
2. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ:КПІ ім. Ігоря Сікорського, 2021. – 258 с.
3. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.
4. Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 «Кібербезпека» / С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
5. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.
6. Mastering Information Security Compliance Management: A comprehensive handbook on ISO/IEC 27001: 2022 compliance.
7. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement Hardcover – Illustrated, March 30 2009 by W. Krag Brotby CISM.

Допоміжна

1. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навчальний посібник. / Національний авіаційний університет; МОН. – К.: НАУ, 2006. – 108 с.
2. Міжнародний стандарт ISO 27001 ISO/IEC 27001 Information technology Security techniques. Information security management systems. Requirements.
3. Міжнародний стандарт ISO/IEC 27000 Information technology Security techniques. Information security management systems. Overview and vocabulary.
4. Міжнародний стандарт ISO/IEC 27002 Information technology Security techniques. Code of practice for information security controls.