МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто на засіданні кафедри
Протокол № 9 від 9 лютого 2023 року

м. Кропивницький – 2023

ЗМІСТ

1. Загальна інформація

Назва дисципліни	Менеджмент інформаційної безпеки
Викладач	Босько Віктор Васильович, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/bosko-viktor/
Контактний телефон	+380668408338
E-mail:	Victorvv2@ukr.net
Консультації	Очні консультації згідно розкладу консультацій середа з 13.20 до 14.40 Онлайн консультації за попередньою домовленістю електронною поштою Victorvv2@ukr.net https://meet.google.com/fuy-xfct-wcc

2. Анотація до дисципліни

Дисципліна «Менеджмент інформаційної безпеки» належить до вибіркових навчальних дисциплін забезпечення навчального процесу за освітнім ступенем «Бакалавр» за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології»

Даний курс знайомить студентів із основними питаннями менеджменту інформаційної безпеки, зокрема впровадженням політики інформаційної безпеки; організації інформаційної безпеки, її внутрішньої організації, політику щодо мобільного обладнання та віддаленої роботи; заходами управління ресурсами СУІБ: відповідальності за ресурси СУІБ, класифікації інформації та поводження з носіями; криптографічних засобів захисту, політикою використання криптографічних засобів; заходами фізичної безпеки та безпеки інфраструктури: зони безпеки, обладнання; засобами забезпечення безпеки експлуатації, зокрема безпечні процедури експлуатації та відповідальності, захисту від зловмисного коду, резервне копіювання, ведення журналів аудиту та моніторинг, управління технічною вразливістю, розгляд аудиту інформаційних систем; засобами забезпечення безпеки експлуатації; засобами забезпечення безпеки комунікацій; засобами забезпечення вимог щодо відносин з постачальниками: інформаційна безпека у взаємовідносинах з постачальниками, управління наданням послуг постачальником.

Мета і завдання дисципліни

Мета: Метою вивчення курсу «Менеджмент інформаційної безпеки» є формування комплексу знань щодо основ менеджменту інформаційної безпеки, набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

Основними **завданнями** вивчення дисципліни є формування наступних компетенцій:

Загальні компетенції.Соціальні навички (soft-skills):

Здатність застосовувати знання у практичних ситуаціях.

Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Фахові компетенції (special-skills):

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.

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

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

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням електронних презентацій, поєднуючи із лабораторними заняттями.

Формат очний (offline / Face to face)

Для заочної форми

Під час сесії формат очний (Face to face), у міжсесійний період – дистанційний(online).

5. Результати навчання

Програмні результати вивчення дисципліни:

Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

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

Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації

Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Рекомендації щодо семестру вивчення	6
Спеціальність	125 «Кібербезпека»
Кількість кредитів/годин	6/180
Кількість змістових модулів	2
Нормативна/вибіркова	вибіркова
Лекції	28
Лабораторні роботи	42
Самостійна робота	110
Вид підсумкового контролю: залік	-

7. Пререквізити

Ефективність засвоєння змісту дисципліни «Менеджмент інформаційної безпеки» значно підвищиться, якщо студент попередньо опанував матеріал таких дисциплін як: Історія та культура України, Філософія, Інформаційна безпека держави та Забезпечення інформаційної безпеки держави.

8. Технічне й програмне забезпечення/обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Практичні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517). Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, бажано мати комп'ютерну техніку (з виходом у глобальну мережу) для виконання тестових завдань в системі дистанційної освіти та підготовки (друку) рефератів і самостійних робіт.

Програмне забезпечення	Вільне ПЗ чи ні	Матеріально-технічне забезпечення
		Лекційні заняття проводяться у ауд. 500 обладнаною мультимедійним проектором Epson EB-X41. Лабораторні роботи виконуються у лабораторіях кафедри кібербезпеки та програмного забезпечення, (ауд 501, 505, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету.
GoogleChrome https://play.google.com/store/apps/details?id=com.android.chrome&hl=uk&gl=U	вільне	

9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення.
Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і практичні заняття курсу.
Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ; Кодексу академічної доброчесності ЦНТУ.

10. Навчально - методична карта дисципліни

Тиждень, академічні години	Тема, основні питання	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Завдання, години	Вага оцінки (бал)	Термін виконання
Змістовний модуль 1. Менеджмент інформаційної безпеки.							
Тиждень 1 (за розкладом) 2 години	**Тема 1 - Передумови й основні напрямки розвитку менеджменту в галузі інформаційної безпеки**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: World Wide Web Consortium (W3C) - Консорціум Всесвітньої Павутини 4 год.	4	Самостійна робота Тиж.1-2
Тиждень 1 (за розкладом) 2 години	Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: International Organization for Standardization (ISO) - Міжнародна організація по стандартизації. 4 год.	4	Самостійна робота Тиж.1-2
Тиждень 2 (за розкладом) 2 години	**Тема 2 - Діяльність міжнародних організацій у галузі інформаційної безпеки**	Лекція / Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Internet Security Alliance (ISA) - Альянс з безпеки мережі Інтернет 4 год.	4	Самостійна робота Тиж.1-2
Тиждень 2 (за розкладом) 2 години	Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет. Оформлення та захист.	Лабораторна роботаFace to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: The International Biometric Industry Association (IBIA) - Міжнародна асоціація компаній-виробників біометричного устаткування 4 год.	4	Самостійна робота Тиж.1-2

Тиждень 3 (за розкладом) 2 години	**Тема 3 - Діяльність спеціалізованих міжнародних організацій і об'єднань у галузі інформаційної безпеки**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Програма попереджувальних захисних дій – Microsoft Active Protections Program (MAPP) 4 год.	4	Самостійна робота Тиж.3-4
Тиждень 3 (за розкладом) 2 години	Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Корпорація Cisco Systems 4 год.	4	Самостійна робота Тиж.3-4
Тиждень 4 (за розкладом) 2 години	**Тема 4 - Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Інфраструктура публічних ключів. 4 год.	4	Самостійна робота Тиж.3-4
Тиждень 4 (за розкладом) 2 години	Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. Оформлення та захист.	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Програмна підтримка аналізу ризиків. 4 год.	3	Самостійна робота Тиж.3-4
Тиждень 5 (за розкладом) 2 години	**Тема 5. Управління інформаційною безпекою на державному рівні:загальні принципи і практика України**	Лекція/ Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: X-Force security intelligence team – Дослідницька група X-Force 4 год.	3	Самостійна робота Тиж.5-6

Тиждень 5 (за розкладом) 2 години	Моніторинг згадувань об'єктів (інцидентів з інформаційною безпекою) у мережі Інтернет	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Сучасні технології захисту інформації. 4 год.	3	Самостійна робота Тиж.5-6
Тиждень 6 (за розкладом) 2 години	**Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Типи закладних пристроїв 4 год.	3	Самостійна робота Тиж.5-6
Тиждень 6 (за розкладом) 2 години	Моніторинг згадувань об'єктів (інцидентів з інформаційною безпекою) у мережі Інтернет. Оформлення та захист.	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Вивчити можливі канали несанкціонованого витоку інформації 4 год.	3	Самостійна робота Тиж.5-6
Тиждень 7 (за розкладом) 2 години	**Тема 7. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Вивчити методи пошуку закладних пристроїв 4 год.	3	Самостійна робота Тиж.7-8
Тиждень 7 (за розкладом) 2 години	Інформаційне забезпечення кадрового менеджменту служб інформаційної безпеки на підприємстві	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Джерела акустоелектричних перетворювань 4 год.	4	Самостійна робота Тиж.7-8
Максимальна кількість балів за змістовним модулем 1						**50**	

Змістовний модуль 2. Забезпечення національної безпеки в різних сферах діяльності.							
Тиждень 8 (за розкладом) 2 години	**Тема 8. Склад деталізованої політики безпеки**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Особливості захисту від витоку інформації акустоелектричним каналом 4 год.	4	Самостійна робота Тиж.7-8
Тиждень 8 (за розкладом) 2 години	Інформаційне забезпечення кадрового менеджменту служб інформаційної безпеки на підприємстві. Оформлення та захист.	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Типи нелінійних локаторів 4 год.	4	Самостійна робота Тиж.7-8
Тиждень 9 (за розкладом) 2 години	**Тема 9. Департамент інформаційної безпеки і робота з персоналом**	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Загрози витоку інформаці 4 год.	4	Самостійна робота Тиж.9-10
Тиждень 9 (за розкладом) 2 години	Організація діяльності відділу управління інформаційними ресурсами та захисту інформації	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Заходи захисту витоку інформації 4 год.	4	Самостійна робота Тиж.9-10
Тиждень 10 (за розкладом) 2 години	**Тема 10. Організація реагування на надзвичайні ситуації (інциденти)**	Лекція / Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Діапазон робочих частот ПК 4 год.	4	Самостійна робота Тиж.9-10

Тиждень 10 (за розкладом) 2 години	Організація діяльності відділу управління інформаційними ресурсами та захисту інформації. Оформлення та захист.	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Заходи захисту серверних 4 год.	4	Самостійна робота Тиж.9-10
Тиждень 11 (за розкладом) 2 години	**Тема 11. Аудит стану інформаційної безпеки на підприємстві** .	Лекція Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Вимоги до серверних приміщень 4 год.	4	Самостійна робота Тиж.11-12
Тиждень 11 (за розкладом) 2 години	Планування заходів аудиту інформаційної безпеки	Лабораторна робота Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Екранування приміщень 4 год.	3	Самостійна робота Тиж.11-12
Тиждень 12 (за розкладом) 2 години	**Тема 12. Програмні засоби, що підтримують управління інформаційною безпекою на підприємстві**	Лекція / Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Технічні засоби виявлення ПЕМВН 4 год.	3	Самостійна робота Тиж.11-12
Тиждень 12 (за розкладом) 2 години	Планування заходів аудиту інформаційної безпеки. Оформлення та захист.	Лабораторна робота / Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Біометричні характеристики людини 4 год.	3	Самостійна робота Тиж.11-12

Тиждень 13 (за розкладом) 2 години	**Тема 13. Надання послуг в сфері інформаційної безпеки**	Лекція / Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Біометричні системи та технології 4 год.	3	Самостійна робота Тиж.13-14
Тиждень 13 (за розкладом) 2 години	Аналіз ринку аудиторських послуг в Україні	Лабораторна робота / Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Основні біометричні параметри 4 год.	3	Самостійна робота Тиж.11-12
Тиждень 14 (за розкладом) 2 години	**Тема 14. Економіка інформаційної безпеки**	Лекція / Face to face	Курс Лекцій http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Ідентифікація людини за допомогою відбитків пальців 3 год.	3	Самостійна робота Тиж.11-12
Тиждень 14 (за розкладом) 2 години	Аналіз ринку аудиторських послуг в Україні. Оформлення та захист.	Лабораторна робота / Face to face	Методичні вказівки до виконання ЛР http://moodle.kntu.kr.ua/course/view.php?id=669#section-15	Базова 1-5 Допоміжна 1-4. Інформаційні ресурси 1-6	Самостійно опрацювати: Ідентифікація людини за допомогою її очей 3 год.	4	Самостійна робота Тиж.11-12
Максимальна кількість балів за змістовним модулем 2						**50**	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, письмовий контроль, тестовий контроль. Форма підсумкового контролю: екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Менеджмент інформаційної безпеки» здійснюється згідно з кредитною трансфернонакопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та

самостійної роботи, лабораторних робіт та індивідуальних завдань), для оцінювання якої призначається максимум 60 балів у семестрі та максимум 40 балів за екзамен.

Змістовний модуль 1														Змістовний модуль 2													
Т1		Т2		Т3		Т4		Т5		Т6		Т7		Т8		Т9		Т10		Т11		Т12		Т13		Т14	
Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР	Л	ЛР
4	4	4	4	4	4	4	3	3	3	3	3	3	4	4	4	4	4	4	4	4	3	3	3	3	3	3	4

Шкала оцінювання: національна та ЄКТС

Оцінка за шкалою ЄКТС	Визначення	Оцінка		
		За національною системою (екзамен, диф. залік, курс. проект, курс. робота, практика)	За національною системою (залік)	За системою ЦНТУ
A	ВІДМІННО - відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	Зараховано	90-100
B	ДУЖЕ ДОБРЕ - вище середнього рівня з кількома помилками	4 (добре)	Зараховано	82-89
C	ДОБРЕ - в загальному правильна робота з певною кількістю грубих помилок			74-81
D	ЗАДОВІЛЬНО - непогано, але зі значною кількістю недоліків	3 (задовільно)	Зараховано	64-73
E	ДОСТАТНЬО - виконання задовольняє мінімальні критерії			60-63
FX	НЕЗАДОВІЛЬНО - потрібно попрацювати перед тим, як перескласти	2 (незадовільно)	Незараховано	35-59
F	НЕЗАДОВІЛЬНО - необхідна серйозна подальша робота			1-34

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, практичні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті: оцінку «відмінно» (90-100 балів, А) заслуговує студент, який:

- всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;
- вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;
- засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;
- засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;
- вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;
- самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку «добре» (82-89 балів, В) - заслуговує студент, який:

- повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

- має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

- під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу; оцінку «добре» (74-81 бал, C) заслуговує студент, який:

- в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;

- вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

- опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) - заслуговує студент, який:

- знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

- виконує завдання, але при рішенні допускає значну кількість помилок;

- ознайомлений з основною літературою, яка рекомендована програмою;

- допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення. оцінку «задовільно» (60-63 бали, E) - заслуговує студент, який:

- володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) - виставляється студенту, який:

виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку «незадовільно» (35 балів, F) - виставляється студенту, який:

- володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

- допускає грубі помилки при виконанні завдань, передбачених програмою;

- не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

Підсумкова (загальна оцінка) курсу навчальної дисципліни. Є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове тестування рівня засвоєності теоретичного матеріалу під час аудиторних занять та самостійної роботи (модульний контроль); оцінка (бали) за виконання практичних індивідуальних завдань. Підсумкова оцінка виставляється після повного вивчення навчальної дисципліни, яка виводиться як сума проміжних оцінок за змістові модулі. Остаточна оцінка рівня знань складається з рейтингу з навчальної роботи, для оцінювання якої призначається 60 балів, та оцінки на екзамені – максимуму 40 балів.

12. Рекомендована література

Базова

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. –Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.
2. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s
3. 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
4. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 - 216 с.

Допоміжна

1. Моделювання економічної безпеки: держава, регіон, підприємство :[монографія] / [Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. та ін.] ; за ред. Гейця В. М. – Х. : ВД "ІНЖЕК", 2006. – 240 с
2. Мунтіян В. І. Економічна безпека України : [підруч.] / В. І. Мунтіян. – К. :КВІСТ, 1999. – 457 с.
3. Аристотель. Політика / Пер. з давньогр. та передм. О. Кислюка. Київ: Основа, 2000. 239 с.
4. Василенко В.Збройна агресія Росії проти України: геополітичний та національний виміри // Юридичний вісник України.№ 42 (1007). 18–24 жовтня 2014. С. 6–7.

Інформаційні ресурси

1. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.
2. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.
3. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.
4. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки.

5. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с. – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf .
6. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf.