

## СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Управління інцидентами інформаційної безпеки»

<b>Лектор курсу</b>		<b>Якименко Юрій Михайлович</b> , кандидат військових наук, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою		<b>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</b>		<b>e-mail:</b> <a href="mailto:yakum14@ukr.net">yakum14@ukr.net</a> ; <b>сторінка курсу в Moodle –</b> <a href="https://dn.dut.edu.ua/course/view.php?id=409">https://dn.dut.edu.ua/course/view.php?id=409</a> <a href="https://dut.edu.ua/uploads/p_284_15032710.pdf">https://dut.edu.ua/uploads/p_284_15032710.pdf</a>	
<b>Галузь знань</b>		12 Інформаційні технології		<b>Рівень вищої освіти</b>		магістр	
<b>Спеціальність</b>		125 Кібербезпека		<b>Семестр</b>		9	
<b>Освітня програма</b>		КІБЕРБЕЗПЕКА		<b>Тип дисципліни</b>		Вибіркова	
<b>Обсяг:</b>	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	6	180	18	-	36	-	126

### АНОТАЦІЯ КУРСУ

<b>Мета курсу:</b>	Формування у студентів знань та умінь, необхідних для організації управління інцидентами, які є основою забезпечення інформаційної безпеки підприємств.
--------------------	---

### Компетентності відповідно до освітньої програми

#### Інтегральна компетентність

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки

Загальні компетентності (КЗ)	Фахові компетентності (КФ)
<p><b>КЗ1.</b> Здатність застосовувати знання у практичних ситуаціях.</p> <p><b>КЗ6.</b> Здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.</p>	<p><b>КФ2.</b> Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.</p> <p><b>КФ4.</b> Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.</p> <p><b>КФ7.</b> Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.</p> <p><b>КФ9.</b> Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.</p>

### Програмні результати навчання (РН)

- РН4.** Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
- РН6.** Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- РН7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
- РН8.** Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
- РН9.** Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
- РН10.** Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- РН12.** Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
- РН14.** Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.
- РН16.** Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
- РН21.** Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
- РН28.** Здатність використовувати професійно профільні знання, готувати та приймати управлінські рішення у сфері інформаційної безпеки.
- РН29.** Уміти застосовувати системний підхід для побудови системи управління (менеджменту) інформаційною безпекою організації (підприємства), яка визначає загальну організацію і класифікацію системи даних, систему доступу, напрямки планування, відповідальність співробітників, використання оцінки ризиків, тощо в контексті інформаційної безпеки.

### ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
<b>Розділ 1 «ПОБУДОВА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІБ НА ОСНОВІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»</b>			
Тема 1. <i>Управління інцидентами в системі забезпечення інформаційної безпеки організації</i> <b>Знати:</b> підходи до побудови ефективної системи інформаційної безпеки (ІБ), кращі практики щодо управління інцидентами ІБ, методика оцінки ефективності СМІБ по реакції на інциденти ІБ, вимоги міжнародних та вітчизняних документів з питань управління інцидентами ІБ, можливості використання процесного підходу до	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Експрес-опитування студентів
	Практичне заняття 1		Аналіз причин інцидентів інформаційної безпеки, пов'язані з роботою персоналу та їх розслідування.
	Практичне заняття 2		Використання процесного підходу до управління інцидентами

<p>управління інцидентами, досвід виконання вимог міжнародних документів щодо організації побудови процесу управління інцидентами в Україні.</p> <p><b>Вміти:</b> розпізнавати виникнення інцидентів інформаційної безпеки та їх розслідування на прикладах.</p> <p><b>Формування компетенцій:</b> К3 1, КФ2, КФ4</p> <p><b>Результати навчання:</b> РН7, РН12, РН29</p> <p><b>Рекомендовані джерела:</b> 1,3,5,8,10,13,16,20</p>	Практичне заняття 3		Методика оцінки ефективності СМІБ по реакції на інциденти інформаційної безпеки
	Практичне заняття 4		Змістовий контроль №1. Виконання кваліфікаційних завдань
<p>Тема 2. <b>Побудова та впровадження комплексної системи управління інцидентами інформаційної безпеки</b></p> <p><b>Знати:</b> Методику впровадження комплексної системи управління інцидентами ІБ, можливості системи підтримки управління інцидентами та проблемами, можливості використання інтелектуальної системи управління інцидентами інформаційної безпеки та підтримки прийняття рішень, принципи організації реагування на інциденти ІБ та підходи до оцінки інцидентів, структуру відповідальності в системі підтримки управління інцидентами та проблемами, можливості системи автоматизації процесу управління інцидентами ІБ в інформаційній системі, порядок використання моделей управління обробкою інцидентів ІБ.</p> <p><b>Вміти:</b> використовувати системи автоматизації процесу управління інцидентами ІБ в інформаційній системі- на прикладі SIEM, розробляти типові положення про групу реагування на інциденти інформаційної безпеки (ГРІБ).</p> <p><b>Формування компетенцій:</b> К3 1, К3-6, КФ2, КФ4, КФ9</p> <p><b>Результати навчання:</b> РН4, РН16, РН21, РН27, РН28</p> <p><b>Рекомендовані джерела:</b> 1,4,5,6,8,11-13,16,17</p>	Лекція 3	5,5*	Лекція-візуалізація
	Лекція 4		Навчальна дискусія за темою Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу
	Практичне заняття 5		Вирішення практичної задачі- розробка типового положення про ГРІБ
	Практичне заняття 6		Використання системи автоматизації процесу управління інцидентами в інформаційній системі- на прикладі SIEM
	Практичне заняття 7		Змістовий контроль №2. Виконання кваліфікаційних завдань
<p>Тема 3. <b>Виявлення та документування інцидентів інформаційної безпеки</b></p> <p><b>Знати:</b> підходи до створення системи інформаційної підтримки виявлення інцидентів безпеки, можливості підтримки реагування на інциденти ІБ, можливості використання основних систем виявлення й попередження інцидентів, правила звітності про події та інциденти ІБ, вимоги стандартів до розробки і змісту Політики інформаційної безпеки організації, структурно-логічні схеми організації виявлення інцидентів ІБ, підходи до організації документування інцидентів інформаційної безпеки на рівні підприємства.</p> <p><b>Вміти:</b> використовувати захисні заходи і засоби від інцидентів; розробляти Керівництво по обробці інцидентів, пов'язаних з діями внутрішніх зловмисників.</p>	Лекція 5	5,5*	Лекція-візуалізація
	Лекція 6		Лекція-візуалізація з експрес-опитування студентів
	Практичне заняття 8		Аналіз можливостей використання основних систем виявлення й попередження інцидентів інформаційної безпеки
	Практичне заняття 9		Ознайомлення і обговорення кращих політик інформаційної безпеки організації від компаній SANS і ін.
	Практичне заняття 10		Підходи до організації документування інцидентів інформаційної безпеки
	Практичне заняття 11		Змістовий контроль №3. Виконання кваліфікаційних завдань

<p><b>Формування компетенцій:</b> КЗ 1, КФ4, КФ7  <b>Результати навчання:</b> ПРН7, ПРН9, ПРН16,  <b>Рекомендовані джерела:</b> 1,5,10,13,14</p>			
<p><b>Тема 1.</b> Управління інцидентами в системі забезпечення інформаційної безпеки організації  <b>Тема 2</b> Побудова та впровадження комплексної системи управління інцидентами ІБ  <b>Тема 3.</b> Виявлення та документування інцидентів інформаційної безпеки</p>	<p>Самостійна робота</p>		<ol style="list-style-type: none"> <li>1. Концептуальний підхід до побудови ефективної системи інформаційної безпеки.</li> <li>2. Заходи щодо захисту інформації і політика інформаційної безпеки.</li> <li>3. Співвідношення ефективності і рентабельності систем інформаційної безпеки.</li> <li>4. Методика оцінки ефективності СМІБ (СУІБ) по реакції на інциденти.</li> <li>5. Приклади інцидентів інформаційної безпеки та їх причини.</li> <li>6. Управління інцидентами та безпекою бізнесу в методології управління інформаційними технологіями.</li> <li>7. Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами інформаційної безпеки</li> <li>8. Реалізація процесу управління інцидентами і проблеми інформаційної безпеки.</li> <li>9. Управління інцидентами та проблемами в процесах підтримки ІТ-сервісів у відповідності з вимогами бібліотек ІТІЛ.</li> <li>10. Розробка та впровадження комплексної системи управління інцидентами інформаційної безпеки</li> <li>11. Багаторівнева модель в системі підтримки управління інцидентами та проблемами.</li> <li>12. Структурно-логічна схема дій керівництва з управління інцидентами на підприємстві.</li> <li>13. Автоматизація процесу управління інцидентами інформаційної безпеки.</li> <li>14. Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу ISO/IEC та моделі PDCA.</li> <li>15. Процедури ефективної роботи групи реагування на інциденти</li> <li>16. Системи виявлення й попередження вторгнень.</li> <li>17. Звітність про події та інциденти інформаційної безпеки.</li> <li>18. Політика управління інцидентами інформаційної безпеки згідно ISO 27035.</li> <li>19. Організація документування інцидентів інформаційної безпеки.</li> </ol>

**Розділ 2 «РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ»**

<p>Тема 4. <b>Моніторинг подій та реагування на інциденти інформаційної безпеки</b>  <b>Знати:</b> основні вимоги та заходи до моніторингу подій і менеджменту інцидентів інформаційної безпеки, підхід до побудови системи моніторингу ІБ, призначення та принципи побудови систем відображення атак і запобігання вторгнень, організація моніторингу подій та реагування на інциденти ІБ, основні структури SIEM-систем з моніторингу подій ІБ, порядок оцінки ефективності процесу управління інцидентами ІБ, витрати та підходи до оцінки забезпечення інформаційної безпеки, порядок розслідування і запобігання випадків з інцидентами, порядок використання DLP-системи при моніторингу ІБ, вимоги та порядок побудови системи розслідування інцидентів ІБ, , можливості моделей по розслідуванню інцидентів ІБ .  <b>Вміти:</b> використовувати методичні інструменти щодо застосування при розслідуванні інцидентів ІБ.  <b>Формування компетенцій:</b> КЗ 6, КФ4,КФ7  <b>Результати навчання:</b> ПРН8,ПРН12, ПРН14, ПРН21  <b>Рекомендовані джерела:</b> 1,3,4,7,12,20,21</p>	Лекція 7	5,5*	Лекція-візуалізація
	Лекція 8		Експрес-опитування студентів
	Практичне заняття 12		Підхід до побудови системи моніторингу інформаційної безпеки, систем відображення атак і запобігання вторгнень
	Практичне заняття 13		Оцінка можливості моделей по розслідуванню інцидентів інформаційної безпеки
	Практичне заняття 14		Змістовий контроль №4. Виконання кваліфікаційних завдань
<p>Тема 5. <b>Оцінка ефективності та вдосконалення процесу управління інцидентами інформаційної безпеки</b>  <b>Знати:</b> Підходи до розробки та використання метрик інцидентів інформаційної безпеки, вимоги до організації безперервності бізнесу підприємства і управління інцидентами, методології, стандарти і нормативні вимоги в галузі управління безперервністю бізнесу, організацію проведення аудиту інформаційної безпеки ІС, найкращі міжнародні практики щодо управління інцидентами ІБ, вимоги бібліотек ІТІЛ до управління інцидентами, методичні інструменти оцінки ефективності процесу управління інцидентами  <b>Вміти:</b> оцінювати ефективність інцидентів інформаційної безпеки організації за допомогою метрик безпеки.  <b>Формування компетенцій:</b> КЗ 1, КФ2, КФ7, КФ9  <b>Результати навчання:</b> ПРН6-8, ПРН10,ПРН14  <b>Рекомендовані джерела:</b> 1,5,6,9,16,17-19,21</p>	Лекція 9	5,5*	Лекція-візуалізація
	Практичне заняття 15		Аналіз вимог в галузі управління безперервністю бізнесу
	Практичне заняття 16		Оцінювання ефективності інцидентів інформаційної безпеки за допомогою метрик безпеки
	Практичне заняття 17		Навчальна дискусія за темою Структуру системи управління інцидентами інформаційної безпеки ( на прикладі NAU-CERT).
	Практичне заняття 18		Змістовий контроль №5. Виконання кваліфікаційних завдань
<p>Тема 4. Моніторинг подій та реагування на інциденти інформаційної безпеки  Тема 5. Оцінка ефективності та вдосконалення процесу управління інцидентами інформаційної безпеки</p>	Самостійна робота		1. Система моніторингу подій інформаційної безпеки 2. Підходи до побудови та реалізація систем відображення атак і запобігання вторгнень

			<p>3. Досвід з організації моніторингу інцидентів інформаційної безпеки на рівні підприємства</p> <p>4. Типові структури SIEM-систем з моніторингу подій інформаційної безпеки</p> <p>5. Оцінка ефективності процесу управління інцидентами.</p> <p>6. Порушення правил і завдання для успішного розслідування інцидентів інформаційної безпеки</p> <p>7. Роботи, пов'язані з розслідуванням порушень інформаційної безпеки</p> <p>8. Метрики безпеки і їх приклади</p> <p>9. Контрольна карта Шухарта</p> <p>10. Безперервність бізнесу і відновлення після інциденту</p> <p>11. Процес визначення метрик і їх оцінки відповідно до нормативних документів і стандарту ISO 27004</p> <p>12. Особливості методик проведення аудиту інформаційної безпеки</p> <p>13. Особливості управління інцидентами інформаційною безпекою у процесах ITSM</p> <p>14. Заходи з вдосконалення процесу управління інцидентами інформаційної безпеки</p>
--	--	--	--

### МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять.

### ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – Київ : Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с. URL: [https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident\\_15042014.pdf](https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf)
2. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес.– № 1(31). – К.: ДУТ, 2020. – С. 64-69. URL: <http://journals.dut.edu.ua/index.php/emb/article/view/2377/2277>
3. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— Київ : ДУТ, 2015.— 288 с.

4. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. // II Міжнародна науково-практична конференція «Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку», 1 лютого 2021 року.— Київ: ДУТ, 2021.- С. 279-282. URL: [http://www.dut.edu.ua/uploads/n\\_9074\\_59003267.pdf](http://www.dut.edu.ua/uploads/n_9074_59003267.pdf)
5. Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків // Матеріали: Всеукраїнська наукова конференція, Актуальні проблеми кібербезпеки, 27 жовтня 2021. Тези доповідей — Київ: ДУТ, 2021.- С.173-176. URL : [http://www.dut.edu.ua/uploads/p\\_2099\\_79407917.pdf](http://www.dut.edu.ua/uploads/p_2099_79407917.pdf)
6. Суворова О.Р. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. Урок №12. URL: <https://naurok.com.ua/keruvannya-mehanizmami-zahistu-mizhnarodni-standarti-informaciyno-bezpeki-104726.html>
7. Рой Я.В., Мазур Н.П., Складанні П.М. Аудит інформаційної безпеки –основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/23>
8. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою.- Професійний розвиток фахівців у системі освіти дорослих: історія, теорія, технології: програма ІV-ої Всеукраїнської Інтернет-конференції 16 жовтня 2019 р., м. Київ.-/за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. К.: Агроосвіта, 2019.- С.41-43.
9. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес. – № .1 –К.: ДУТ, 2020. – С. 64-69. URL: <http://journals.dut.edu.ua/index.php/emb/article/view/2386>
10. Якименко Ю. М. Методичні підходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави / Ю.М. Якименко // Актуальні проблеми управління інформаційною безпекою держави: XII Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання — Київ: Нац. акад. СБУ, 2021.- С. 162-164. URL: <http://academy.ssu.gov.ua/upload/file/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%2026.03.2021.pdf>
11. Якименко Ю. М. Управління інцидентами інформаційної безпеки в організації системи забезпечення кіберстійкості підприємства. Матеріали Всеукраїнської НПК Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 25 лютого 2021 року. Тези доповідей – Київ: ННІЗІ ДУТ, 2021.- С.24-25. URL: [http://www.dut.edu.ua/uploads/l\\_2173\\_91341086.pdf](http://www.dut.edu.ua/uploads/l_2173_91341086.pdf).
12. Yakymenko, Y., Muzhanova, T., & Lehominova, S. (2021). СИСТЕМНИЙ АНАЛІЗ ТЕХНІЧНИХ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ВІД КОМПАНІЇ FIREEYE. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(12), 36-50. URL : <https://doi.org/10.28925/2663-4023.2021.12.3650>
13. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
14. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014), Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
15. ДСТУ ISO/IEC 27031:2015 (ISO/IEC 27031:2011, IDT) Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу
16. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами.
17. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.
18. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
19. ISO/IEC 27002:2013 Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
20. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою
21. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT) Настанови щодо проведення аудитів систем управління

22. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: [https://dut.edu.ua/uploads/1\\_2230\\_88161692.pdf](https://dut.edu.ua/uploads/1_2230_88161692.pdf) .

## ПОЛІТИКА КУРСУ

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за виконане завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

## \*КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 35 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
<b>ПОТОЧНИЙ КОНТРОЛЬ</b>	<i>Робота на заняттях, у т.ч.:</i>	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 балів
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
<b>РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)</b>	Змістовий контроль № 1	максимальна оцінка – 7 балів
	Змістовий контроль № 2	максимальна оцінка – 7 балів
	Змістовий контроль № 3	максимальна оцінка – 7 балів
	Змістовий контроль № 4	максимальна оцінка – 7 балів
	Змістовий контроль № 5	максимальна оцінка – 7 балів
<b>Додаткова оцінка</b>	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку



<b>ПІДСУМКОВЕ ОЦІНЮВАННЯ</b> <i>Залік</i>	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	35 балів
--	---	----------

**ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ**

бали	Критерії оцінювання	Рівень компетентності	Оцінка /зapis в екзаменаційній відомості
90-100	<p>Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях.</p> <p>Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь.</p> <p>Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.</p>	<p><b>Високий</b></p> <p>Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.</p>	Відмінно / Зараховано (А)
82-89	<p>Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.</p> <p>Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.</p>	<p><b>Достатній</b></p> <p>Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни</p>	Добре / Зараховано (В)
75-81	<p>Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності.</p> <p>Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.</p>	<p><b>Достатній</b></p> <p>Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.</p>	Добре / Зараховано (С)
64	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою	<b>Середній</b>	Задовільно /

	дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	<b>Середній</b> Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	<b>Низький</b> Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	<b>Незадовільний</b> Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не представляється