ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 12 «МОНІТОРИНГ, АУДИТ ТА УПРАВЛІННЯ СИСТЕМАМИ КІБЕРБЕЗПЕКИ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
Володимир ВОРОТНІКОВ

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки Єлизавета БАЙЛЮК, кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність 125 «Кібербезпека»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 4</td><td>1-й</td><td>–</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td>2-й</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: аудиторних 3</td><td rowspan="10">Освітній ступінь «магістр»</td><td>16 год.</td><td>4</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>6</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>80</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен, курсова робота</td></tr>
</table>

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання − 11 % аудиторних занять, 89 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Моніторинг, аудит та управління системами кібербезпеки» є формування розуміння студентами теоретичних основ та набуття знань і практичних умінь про сучасні наукові концепції, поняття, принципи та методи моніторингу і аудиту кібербезпеки, процедури управління інцидентами інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів, що є професійною основою для фахівця в галузі управління інформаційною безпекою.

Завданнями вивчення навчальної дисципліни «Моніторинг, аудит та управління системами кібербезпеки» є набуття знань, умінь та навичок (компетентностей), спрямованих на:

- знання сучасних методів та технологій забезпечення безпеки інформаційно-комунікаційних систем кібербезпеки;
- здатність аналізувати та визначати зовнішні та внутрішні загрози в межах інформаційно-комунікаційних систем;
- здатність супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційно-комунікаційних систем;
- вміння інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі моніторингу, аудиту та управління системами кібербезпеки.

Зміст навчальної дисципліни «Моніторинг, аудит та управління системами кібербезпеки» направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інфорації»:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КФ-2. 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.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ-4. 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.

КФ-5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-9. 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.

Отримані знання з навчальної дисципліни «Моніторинг, аудит та управління системами кібербезпеки» стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека та захист інформації»:

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН-5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-9. Аналізувати, розробляти і супроводжувати систему управління інформаційною

безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН-12. 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.

РН-14. 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.

РН-16. 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.

РН-19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН-23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи моніторингу, аудиту та управління системами кібербезпеки.

Тема 1. Основні поняття моніторингу, аудиту та управління системами кібербезпеки.

1. Знайомство з SOC.
2. Вступ до SIEM та SOAR.
3. Функції та завдання синьої команди.
4. Функції та завдання червоної команди.
5. Огляд безпеки DevOps.

Тема 2. Операції безпеки та ландшафт загроз.

1. Розуміння ландшафту загроз.
2. Підвищення привілеїв.
3. Віддалене виконання коду.

Тема 3. Аналіз операційних систем.

1. Збір та фільтрація подій операційної системи Windows за допомогою Procmon.
2. Windows – журнали подій: запити та фільтри PowerShell.
3. Передача хешу в операційній системі Windows.
4. Збір інформації про операційну систему Linux.
5. Системний журнал операційної системи Linux.

Тема 4. Аналіз шкідливих програм.

1. Аналіз зловмисного програмного забезпечення: ознайомлення з основними інструментами.
2. Розширення браузера Recorded Future.
3. Аналіз шкідливих програм: VirusTotal.
4. Windows – аналіз заголовків електронної пошти.
5. Windows – аналіз URL-адрес електронної пошти.

Змістовий модуль 2. Моніторинг мережі, аналіз журналів подій та пошук шкідливого програмного забезпечення.

Тема 5. SIEM – використання Splunk для ефективного моніторингу різних джерел журналів і типів даних.

1. Splunk: основи.
2. Splunk: фільтри та запити.
3. Splunk: поля та трансформації.
4. Splunk: Візуалізації.
5. Splunk: Сповіщення.

Тема 6. Пошук шаблонів за допомогою регулярних виразів і в рамках правил YARA.

1. Огляд YARA.
2. Регулярні вирази в YARA.
3. Управління правилами YARA.
4. Генерація правил YARA.
5. Написання правил YARA.

Тема 7. Аналіз мережі.

1. Основи Wireshark.
2. Основи Suricata.
3. Suricata: правила IDS.
4. Suricata: керування правилами.

Тема 8. Сценарії.

1. Базовий сценарій оболонки.
2. Windows – Основи PowerShell.

Змістовий модуль 3. Запобігання вторгненням в ІКС та управління вразливими місцями.

Тема 9. Керування журналами.

1. Windows – журналювання PowerShell.
2. Керування журналами Linux: журнал Systemd.
3. Splunk: Конфігурація введення.
4. Основи Splunk API.

Тема 10. Політика безпеки.

1. Windows – керування правами Active Directory.
2. Windows – групова політика для пересилання подій з робочої станції

Active Directory GPO.

3. Windows – слабкі та повторно використані облікові дані.
4. Windows – хеші NTLM.
5. Протокол Traffic Light.

Тема 11. Виявлення та запобігання вторгненням.

1. Криміналістика PCAP: Wireshark.
2. Suricata: правила IPS.
3. Криміналістика PCAP – дешифрування та аналіз HTTPS/TLS.
4. Розслідування з Wireshark.
5. Політики брандмауера: FortiOS.

Тема 12. Управління вразливими місцями.

1. Основи веб-сканера Nikto.
2. Використання інструменту Sudo Killer в операційній системі Linux.
3. Управління вразливістю Greenbone.
4. Набір стандартів OpenSCAP.

Змістовий модуль 4. Управління мережевою безпекою.

Тема 13. Індикатори компромісу.

1. Візуальний спуфінг.
2. Ідентифікація IOC Linux.
3. Сканер LOKI IOC.
4. Windows – ІК процес впровадження (Splunk).
5.

Тема 14. IBM QRadar.

1. Огляд QRadar.
2. QRadar: основи.
3. QRadar: мережева активність.
4.

Тема 15. Програми-вимагачі.

1. Огляд програм-вимагачів.
2. Еволюція програм-вимагачів.
3. Знайомство з програмами-вимагачами Ryuk, RansomEXX, REvil, BlackMatter, Hades Ransomware, Egregor Ransomware, DoppelPaymer, Conti Ransomware.

Тема 16. Безпека облікових даних.

1. Злом паролів.
2. Захист від атак методом «грубої сили».
3. Виявлення ескалації привілеїв.
4.

Змістовий модуль 4. Курсова робота

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	лабораторні	самостійна робота
Змістовий модуль 1. Основи моніторингу, аудиту та управління системами кібербезпеки.								
Тема 1. Основні поняття моніторингу, аудиту та управління системами кібербезпеки	5	1	2	2	5	1	2	2
Тема 2. Операції безпеки та ландшафт загроз.	5	1	2	2	5			5
Тема 3. Аналіз операційних систем.	6	1	2	3	6			6
Тема 4. Аналіз шкідливих програм.	6	1	2	3	6			6
Разом за змістовий модуль 1	22	4	8	10	22	1	2	19
Змістовий модуль 2. Моніторинг мережі, аналіз журналів подій та пошук шкідливого програмного забезпечення.								
Тема 5. SIEM – використання Splunk для ефективного моніторингу різних джерел журналів і типів даних.	5	1	2	2	5	1	2	2
Тема 6. Пошук шаблонів за допомогою регулярних виразів і в рамках правил YARA.	5	1	2	2	5			5
Тема 7. Аналіз мережі.	6	1	2	3	6			6
Тема 8. Сценарії.	6	1	2	3	6			6
Разом за змістовий модуль 2	22	4	8	10	22	1	2	19
Змістовий модуль 3. Запобігання вторгненням в ІКС та управління вразливими місцями.								
Тема 9. Керування журналами.	5	1	2	2	5	1	2	2
Тема 10. Політика безпеки.	5	1	2	2	5			5
Тема 11. Виявлення та запобігання вторгненням.	6	1	2	3	6			6
Тема 12. Управління вразливими місцями.	6	1	2	3	6			6
Разом за змістовий модуль 3	22	4	8	10	22	1	2	19
Змістовий модуль 4. Управління мережевою безпекою.								
Тема 13. Індикатори компромісу.	6	1	2	3	6	1		5
Тема 14. IBM QRadar.	6	1	2	3	6			6
Тема 15. Програми-вимагачі.	6	1	2	3	6			6
Тема 16. Безпека облікових даних.	6	1	2	3	6			6
Разом за змістовий модуль 4	24	4	8	12	24	1	0	23
ВСЬОГО	90	16	32	42	90	4	6	80

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Дослідження загроз, вразливостей та атак в межах інформаційних систем.	2	–
2	Дослідження інструментів журналювання подій операційної системи Windows.	2	–
3	Дослідження інструментів журналювання подій операційної системи Linux.	2	–
4	Дослідження інструментів та програмного забезпечення для аналізу шкідливих програм.	2	–
5	Дослідження інструмента YARA для виявлення та класифікації шкідливого програмного забезпечення.	2	–
6	Моніторинг мережі за допомогою Wireshark.	2	–
7	Дослідження роботи системи виявлення і попередження мережевих вторгнень Suricata.	2	–
8	Дослідження системного менеджера Systemd операційної системи Linux.		
9	Дослідження роботи системи зберігання та аналізу логів Splunk.	2	–
10	Дослідження групової політики для пересилання подій з робочої станції Active Directory GPO.	2	–
11	Дослідження FortiOS для захисту гібридних мереж, кінцевих точок та хмарних розгортань у рамках системи Fortinet Security Fabric.	2	–
12	Дослідження веб-сканера Nikto для перевірки цільового веб-сервера на наявність небезпечних файлів та сценаріїв, інструментів адміністрування базами даних, застарілого програмного забезпечення.	2	–
13	Використання інструменту Sudo Killer в операційній системі Linux.	2	–
14	Дослідження сканера LOKI IOC для виявлення зараження системи, підозрілих об'єктів та ознак компроментації або злому комп'ютера чи мережі.	2	–
15	Дослідження IBM QRadar для управління мережевою безпекою.	2	–
16	Дослідження програм-вимагачів.	2	–
РАЗОМ		32	–

6. Завдання для самостійної роботи

Тема 1. Системи аудиту інформаційної безпеки.

1. Основні положення.
2. Термінологія аудиту.

3. Основні види аудиту інформаційної безпеки. Експертний аудит. Активний аудит. Аудит на відповідність стандартам інформаційної безпеки.

4. Діагностичний аналіз Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.

Тема 2. Внутрішній аудит СМІБ.

1. Завдання аудиту. Мета аудиту. Склад процедури аудиту. Критерії аудиту. Процес усвідомлення аудиту інформаційної безпеки. Програма аудиту інформаційної безпеки. Принципи проведення аудиту.

2. Стандарт CobiT 4.1. Бібліотека інфраструктури інформаційних технологій – ITIL. Стандарт ISO/IEC 15408. Серія стандартів ISO/IEC 2700X.

3. Загальна характеристика внутрішніх аудитів СМІБ. Принципи проведення внутрішнього аудиту. Алгоритм організації та проведення внутрішніх аудитів. Пошук загроз. Моделювання загроз.

4. Позаплановий внутрішній аудит. Приклад вимог до процедур з внутрішнього аудиту. Принципи проведення внутрішнього аудиту. Дев’ять правил успішного проведення аудиту. Управління програмою аудиту. Розробка цілей програми аудиту. Розробка програми аудиту.

Тема 3. Комплексний аудит інформаційної безпеки

1. Компетентність особи, що здійснює управління програмою аудиту.

2. Встановлення обсягу програми аудиту. Виявлення та оцінювання ризиків для програми аудиту.

3. Розробка процедур для програми аудиту. Визначення ресурсів, необхідних для реалізації програми аудиту. Реалізація програми аудиту. Вибір методів проведення аудиту. Формування команди з аудиту.

4. Моніторинг програми аудиту. Аналіз та удосконалення програми аудиту.

Тема 4. Оцінка діяльності з управління інформаційною безпекою організації.

1. Встановлення цілей, сфери та критеріїв для конкретного аудиту.

2. Покладання відповідальності на керівника команди з аудиту за конкретний аудит.

3. Управління результатами реалізації програми аудиту. Використання записів відповідно до програми аудиту та їх збереження.

4. Специфічні знання та навички аудиторів, пов'язані з особливостями систем менеджменту і галузями економіки.

Тема 5. Базові принципи, терміни та визначення системи менеджменту інцидентами інформаційної безпеки (СМІІБ).

1. Цілі управління інцидентами.

2. Основні заходи створення СМІБ.

3. Ознаки інциденту інформаційної безпеки. Аналіз інцидентів інформаційної безпеки.

Тема 6. Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки.

1. Визначення показників ефективності процесу управління інцидентами інформаційної безпеки.

Тема 7. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.

1. Етапи формування СМІБ відповідно до моделі PDCA.
2. Модель життєвого циклу процесу УІБ.
3. Усунення причин, наслідків інциденту і його розслідування.

Тема 8. Особливості менеджменту інцидентів відповідно до ITIL

1. Місце процесу управління інцидентами серед усіх процесів ITIL.
2. Основні етапи управління інцидентами відповідно до ITIL. Варіанти категорування інцидентів відповідно до ITIL.

Тема 9. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.

1. Інтеграційна платформа автоматизованої системи управління інцидентами інформаційної безпеки.
2. Апаратно-програмні засоби моніторингу і аудиту.
3. Апаратно-програмні засоби захисту.
4. Сховище інформації про ІІБ.
5. Аналітичні інструменти і засоби генерації звітів.

Тема 10. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

1. Загальна характеристика діяльності груп CERT/CSIRT.
2. Етапи створення груп CERT/CSIRT.
3. Сервіси, що надаються групами реагування на інциденти інформаційної безпеки.
4. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT.
5. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

7. Індивідуальні завдання

Індивідуальні завдання з дисципліни полягають у виконанні лабораторних робіт згідно варіанту по списку в журналі та відпрацюванні матеріалу навчальних курсів мережевої академії Cisco NetAcad та інтерактивної та практичної платформи командної кіберготовності RangeForce.

8. Методи навчання

В ході вивчення дисципліни використовуються наступні методи навчання: мультимедійні презентації, аналіз інформації з відкритих джерел, комп’ютерне моделювання, статистичний аналіз.

Основними видами занять, які проводяться під керівництвом викладача, є лекції, лабораторні роботи та самостійна робота.

На лекціях розглядаються загальні теоретичні положення дисципліни. Під час проведення лекцій використовуються мультимедійні засоби для інтерактивної демонстрації прикладів та графічного матеріали. До кожної лекції студентам додається презентація основних положень.

При виконанні лабораторних робіт зміцнюються знання, отримані на лекціях, набуваються первинні навички з проведення розрахунків міцності захисту, створення моделі загроз та моделі порушника, комп’ютерного моделювання загроз за допомогою різного програмного забезпечення, реалізації моделей контролю доступу до інформації з обмеженим доступом.

При самостійній роботі студенти набувають навички самостійного освоєння матеріалу, який не використаний в навчальному процесі.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль. Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль. Оцінюється вхідний, проміжний, кінцевий рівень знань студента. Підсумковий контроль проводиться у вигляді комп’ютерних тестів та/або виконання практичних завдань.

10. Розподіл балів

Поточне тестування та самостійна робота								Сума
Змістовий модуль 1				Змістовий модуль 2				
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	100
6	6	6	7	6	6	6	7	
Змістовий модуль 3				Змістовий модуль 4				
Т9	Т2	Т3	Т4	Т5	Т6	Т7	Т8	
6	6	6	7	6	6	6	7	

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Bejtlich, Richard.The practice of network security monitoring : understanding incident detection and response, No Starch Press, Inc.38 Ringold Street, San Francisco, CA 94103, 2013, 380p.

2. Elisa Bertino, Kenji Takahashi. Identity Management. Concepts, Technologies, and Systems. Boston: ARTECH HOUSE, 2011. 198 p.

3. Guidelines for auditing management systems : ISO 9011:2011 // International Organization for Standardization (ISO). – 2011. – 52 p.

4. Vinh Hoa La. Security monitoring for network protocols and applications. Networking and Internet Architecture [cs.NI]. Université Paris-Saclay, 2016., 130p.

5. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки// О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

6. Навчальний курс SOC Analyst 1. [Електронний ресурс] – rangeforce.com

7. Навчальний курс SOC Analyst 2. [Електронний ресурс] – rangeforce.com

Допоміжна література

1. Покроковий посібник по створенню CSIRT / ENISA (в рамках програми WP- 2006). – 2006. – 86 с.
2. Information technology. Security techniques. Information security management. Measurement : ISO/IEC 27004:2009 / International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2009. – 55 p.
3. Information technology. Security techniques. Information security incident management : ISO 27035:2011. – 78 p.
4. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira JW-B., Stikvoort D., Kossakowski K.-P. et al. – Pittsburgh, 2003. – 223p.
5. Performance Measurement Guide for Information Security: NIST Special Publication 800-55- rev1. / U.S. Government Printing Office. Washington – 2008. – 80 p.

12. Інформаційні ресурси в Інтернеті

Новітні теоретичні та практичні дані й матеріали що стосуються теорії та практики моніторингу, аудиту та управління системами кібербезпеки рекомендується відслідковувати засобом звертання до наступних сайтів:

1. https://tzi.com.ua/audbezib.html
2. https://portal.rangeforce.com/
3. https://www.netacad.com/
4. http://www.crest-approved.org
5. https://www.iso27001security.com
6. https://securityonion.net/
7. http://www.enisa.europa.eu
8. https://www.splunk.com