ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«30» червня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Рівень вищої освіти	**другий (магістерський) рівень**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Освітня програма	**Безпека інформаційних та комунікаційних систем**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2023

Робоча програма навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації** освітньої програми **Безпека інформаційних та комунікаційних систем**

Розробники: Чобаль О.І., к. ф.-м. н., доцент кафедри ТЕІБ; Фролов А.О., асистент кафедри ТЕІБ

Робочу програму розглянуто та затверджено на засіданні кафедри
твердотільної електроніки та інформаційної безпеки

протокол № 9 від «15» червня 2023 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «28» червня 2023 р.

Голова науково-методичної комісії _____ Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3,5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 105</td><td>1-й</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для денної форми навчання:

аудиторних – 3

самостійної роботи студента – 4</td><td>2-й</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>24</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>Вид підсумкового контролю: іспит</td><td></td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>63</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем» 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.

.

Завданнями даного курсу є набуття знань, умінь та навичок (компетентностей), спрямованих на:

− знання сучасних методів та технологій забезпечення безпеки інформаційно-комунікаційних систем кібербезпеки;

− 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.

Місце дисципліни в структурі освітньої програми: навчальна дисципліна **«Моніторинг та аудит інформаційно-комунікаційних систем»** є обов'язковим компонентом циклу професійної підготовки освітньої програми підготовки магістрів спеціальності «Безпека інформаційних та комунікаційних систем».

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

Інтегральна: здатність розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність оцінювати та забезпечувати якість виконуваних робіт (КЗ-4).
3. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності) (КЗ-6).

Фахові компетентності:

1. 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 (КФ4).
2. 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 (КФ5).
3. 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 (КФ9).

Передумовою вивчення навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** є опанування навчальної дисципліни (НД) “Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки” згідно структурно-логічної схеми даної освітньої програми (ОП).

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **Безпека інформаційних та комунікаційних систем** вивчення навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	**Шифр ПРН**
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	ПРН 8
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ПРН 9
Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	ПРН 10
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	ПРН 14
Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	ПРН 15
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.	ПРН 16
Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	ПРН 18
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.	ПРН 19
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.	ПРН 23
Володіти методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно- комунікаційних системах.	ПРН 24

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** є:

- іспит;
- виконання завдань практичних та лабораторних робіт;
- стандартизовані тести;
- фронтальне та/або письмове опитування

Форми контролю та критерії оцінювання результатів навчання

Модульний контроль з навчальної дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** складається з поточного контролю та модульного контрольного оцінювання результатів навчання.

Форми поточного контролю:

- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- захист результатів лабораторної роботи;
- тестування;
- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів.

Форма модульного контрольного оцінювання: письмова модульна контрольна робота та/або тестування.

Форма підсумкового семестрового контролю: іспит.

До іспиту допускаються студенти, які відпрацювали пропущені заняття і виконали модульні контрольні роботи та завдання для самостійної роботи. Контроль самостійної роботи здійснюється шляхом перевірки виконаних завдань на практичних та індивідуальних заняттях, під час захисту лабораторних робіт, тестування при поточному оцінюванні, презентації результатів виконаних завдань та досліджень.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточний контроль успішності					**Модульна контрольна робота**	**Сума**
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	5	10	15	5		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточний контроль успішності					Модульна контрольна робота	Сума
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
10	5	5	5	15		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни «Автоматизація обробки інформації з обмеженим доступом»

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні та семінарські заняття	5	25	3	15
Комп'ютерне тестування при тематичному оцінюванні	1	15	1	25
Модульна контрольна робота	1	60	1	60
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом відповідей на питання навчального модуля та вирішення тестових завдань. Кожна правильна відповідь оцінюється певною кількістю балів. Максимальна кількість балів за кожний модуль становить 100 балів.

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«Моніторинг та аудит інформаційно-комунікаційних систем»** здійснюється у формі іспиту, що проводиться в усній формі шляхом співбесіди. Результати іспиту оцінюються за чотирибальною шкалою: "відмінно", "добре", "задовільно", "незадовільно". Підсумкова оцінка визначається наступними критеріями:

Оцінки «відмінно» (А) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії.

Оцінки «добре» (В) заслуговує студент, що виявив повне знання програмового матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу, рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до їх самостійного поповнення, але під час відповіді допустив незначні неточності.

Оцінки «добре» (С) заслуговує студент, що виявив повне знання програмового матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу, рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до їх самостійного поповнення, але під час відповіді допустив неточності і помилки.

Оцінки «задовільно» (D) заслуговує студент, що виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка «задовільно» виставляється студентам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення.

Оцінки «задовільно» (E) заслуговує студент, що виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, ця оцінка виставляється студентам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача.

Оцінка «незадовільно» (FX) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань. Студенти, які не з'явилися на екзамен без поважних причин, вважаються такими, що одержали незадовільну оцінку.

Оцінка «незадовільно» (F) виставляється студенту, не виконав повністю план навчальної дисципліни, виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань, не виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією.

За результатами рейтингового контролю знань студентів, дозволяється виставлення екзаменаційної оцінки (без складання іспиту) із відповідною оцінкою за системою ECTS у випадку набору кількості балів, не меншій мінімальній оцінці E з кожного модуля. Студент має право підвищити оцінку за системою ECTS, складаючи іспит. За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-и бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Оцінка за шкалою балів	ECTS	
	Оцінка	Характеристика
90-100	A	відмінно
82-89	B	добре
74-81	C	добре
64-73	D	задовільно
60-64	E	задовільно
35-59	FX	незадовільно з можливістю перескладання
1-34	F	незадовільно з обов'язковим повторним навчанням

Студент, який отримав за результатами підсумкового контролю оцінку «незадовільно з обов'язковим повторним навчанням» (1-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни (під час додаткового семестру) і скласти іспит.

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. МОНІТОРИНГ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Тема 1. Вступ. Поняття про сервіси моніторингу подій кібербезпеки та аудиту інформаційно-комунікаційних систем.
Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Термінологія моніторингу та аудиту ІКС.
Призначення та сфера застосування моніторингу та аудиту. Сучасний стан кіберзагроз. Цілі та підходи щодо забезпечення операційної діяльності кібербезпеки. Основні види аудиту інформаційно-комунікаційних систем .

Тема 2. Кібербезпека і центр моніторингу та управління безпекою (SOC)
Поняття про Security Operations Center (SOC). Елементи центру моніторингу та управління безпекою. Люди, процеси і технології в SOC. Архітектура та інструменти SOC. Breach detection системи. SIEM-системи.

Тема 3. Моніторинг кібербезпеки інформаційно-комунікаційних систем
Моніторинг інформаційно-комунікаційних систем. Моніторинг кібербезпеки інформаційної системи. Моніторинг стану IT систем і мереж з використанням сканерів безпеки. Моніторинг поточного функціонування інформаційно-комунікаційних систем. Реалізація оперативного контролю за діями користувачів.

Тема 4. Моніторинг безпеки мереж (NSM)
Загальні поняття про Network Security Monitoring (NSM). Джерела даних NSM: Flow. Traffic, Transactions, Alerts, Correlated Alerts. Основні можливості NSM: виявлення атаки на стороні клієнта та сервера, відстеження передач файлів, контроль команд та ідентифікація трафіку, виявлення аномалій, мережева інвентаризація. Дизайн та архітектура NSM.

Тема 5. Моніторинг MS Windows
Архітектура та безпека Windows. Нативні журнали та моніторинг Windows. Вдосконалена політика аудиту з політикою Legacy Audit. Моніторинг важливих подій Windows. Аналіз журналу: перегляд подій Windows, Powershell, LogParser. Додаткові джерела логів Windows: Sysmon, Autoruns. Windows Post Exploitation TTP (Persistence, Privilege Escalation, Defense, Execution). Виявлення атак на Microsoft Active Directory.

Модуль 2. АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Тема 1. Аудит інформаційної безпеки інформаційно-комунікаційних систем
Основні види аудиту інформаційної безпеки. Експертний аудит. Активний аудит. Аудит на відповідність стандартам інформаційної безпеки. Діагностичний аналіз Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.

Тема 2. Аудит системи менеджменту інформаційної безпеки
Загальна характеристика внутрішніх аудитів СМІБ. Принципи проведення внутрішнього аудиту. Алгоритм організації та проведення внутрішніх аудитів. Пошук загроз. Моделювання загроз.

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. Процеси ризик-менеджменту в інформаційно-комунікаційних системах
Міжнародні стандарти оцінювання інформаційних ризиків. Сучасні методи і засоби оцінювання ризиків в інформаційно-комунікаційних системах. Сучасні бази даних вразливостей інформаційної безпеки. Оцінювання ризиків інформаційної безпеки. Обробка і прийняття ризиків інформаційної безпеки. Особливості оцінки загроз і ризиків у соціотехнічних системах.

Тема 4. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT в інформаційно-комунікаційних системах
Загальна характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/CSIRT. Сервіси, що надаються групами реагування на інциденти інформаційної та кібербезпеки. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління кіберінцидентами.

Тема 5. Практична методологія IT-аудиту
Основи IT-аудиту. Набір інструментів IT-аудиту для конкретних завдань. Процес і кроки IT-аудиту. Попереднє дослідження об'єкта аудиту та планування внутрішнього аудиту. Проведення аудиту та аналіз. Звітування за результатами IT-аудиту. Відстеження результатів впровадження аудиторських рекомендацій. Забезпечення якості в IT-аудитах

5.2. Структура навчальної дисципліни

Денна форма навчання

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Вступ. Поняття про сервіси моніторингу подій кібербезпеки та аудиту інформаційно-комунікаційних систем.	8	2				6
Тема 2. Кібербезпека і центр моніторингу та управління безпекою (SOC)	10	2	2			6
Тема 3. Моніторинг кібербезпеки інформаційно-комунікаційних систем	12	2	4			6
Тема 4. Моніторинг безпеки мереж (NSM)	12	2	4			6
Тема 5. Моніторинг MS Windows	10	2	2			6
Модульна контрольна робота	2	2				
Разом за модуль	54	12	12			30
Модуль 2						

Тема 1. Аудит інформаційної безпеки інформаційно- комунікаційних систем	10	2	2			6
Тема 2. Аудит системи менеджменту інформаційної безпеки.	9	2				7
Тема 3. Процеси ризик-менеджменту в інформаційно-комунікаційних системах	10	2				8
Тема 4. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT в інформаційно-комунікаційних системах	8	2				6
Тема 5. Практична методологія IT-аудиту	12	2	4			6
Модульна контрольна робота	2	2				
Разом за модуль	51	12	6			33
Разом за семестр	**105**	**24**	**18**			**63**

5.3. Теми практичних занять

№ з/п	Назва теми	Кількість Годин	
		Денна	Заочна
1	Вивчення функціональних можливостей системи виявлення вторгнень Snort	2	
2	Моніторинг ІКС за допомогою Splunk	2	
3	Моніторинг стану IT систем і мереж з використанням сканерів безпеки	4	
4	Моніторинг мережі за допомогою Wireshark	2	
5	Дослідження групової політики для пересилання подій з робочої станції Active Directory GPO	2	
6	Визначення завдань аудиту та технічного стандарту аудитування.	2	
7	Проведення аудиту безпеки інформаційно-комунікаційної системи	4	
	Разом	**18**	

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Призначення та склад системи моніторингу подій інформаційної безпеки (SIEM).	4	
2.	Функції та джерела інформації системи моніторингу подій інформаційної безпеки (SIEM).	4	
3.	Основні механізми перехоплення трафіка	4	
4.	Архітектура і основні типи DLP-систем	4	
5.	Програмні засоби аналізу трафіка	4	
6.	Ключові компоненти протоколу SNMP	4	
7.	SIEM – використання Splunk для ефективного моніторингу різних джерел журналів і типів даних	4	
8.	Пошук шаблонів за допомогою регулярних виразів і в рамках правил YARA	4	
9.	Життєвий цикл реагування на інциденти NIST	4	
10.	Загальна система оцінки вразливостей (Common Vulnerability	4	

	Scoring System, CVSS).		
11.	Дослідження засобів перешкоджання аудиту інформації в IT системі	4	
12.	Аудит цілісності файлових систем	4	
13.	Особливості IT-аудиту в банківських установах	4	
14.	Програмні продукти, призначені для аналізу й керування ризиками.	4	
15.	Особливості менеджменту інцидентів відповідно до ITIL	4	
16.	Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.	3	
	Разом	**63**	

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: технічні засоби навчання, зокрема мультимедійний проектор.
Обладнання: персональні комп'ютери з можливістю доступу в Інтернет (Windows 10, Cisco Packet Tracer, Kali Linux, WireShark, Nessus, Metasploit). Полігон кібербезпеки кафедри ТЕІБ: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2
Інформаційне забезпечення: курс CyberOps Associate (English - 1.02) на порталі Мережевої академії Cisco (філія - Ужгородський національний університет).

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. 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.
2. 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.
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
4. Сертифікований курс англійською мовою CyberOps Associate (English - 1.02) на порталі Мережевої академії Cisco (філія - Ужгородський національний університет).
5. Електронний навчальний курс «Моніторинг і аудит інформаційно-комунікаційних систем» на платформі e-learn.uzhnu.edu.ua для студентів спеціальності 125 Кібербезпека та захист інформації.

Допоміжна література

1. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
2. Кількісна оцінка кіберзахищеності інформації / В. Хорошко, Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
3. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

1. https://www.netacad.com/
2. https://www.splunk.com/
3. https://portal.rangeforce.com/