МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

_____ Каріна НЕМАШКАЛО

ІНЖЕНЕРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**всі**
Спеціальність	**всі**
Освітній рівень	**другий (магістерський)**
Освітня програма	**всі**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Розробник:
к.т.н., доц. _____ Наталія ДОЛГОВА

Завідувач кафедри
кібербезпеки та інформаційних технологій
д.т.н., проф. _____ Ольга СТАРКОВА

Харків
2023

ВСТУП

Актуальність навчальної дисципліни та її необхідність та роль у підготовці фахівців полягає у її орієнтованості на сучасні ефективні технічні та організаційні заходи для захисту конфіденційної інформації та інформаційно-комунікаційних систем від зловмисних атак, застосування яких дає змогу розв'язувати завдання кібербезпеки мереж.

Метою навчальної дисципліни “Інженерія безпеки інформаційно-комунікаційних систем” є навчання здобувачів вищої освіти принципам побудови комплексних систем захисту інформації для формування контуру безпеки бізнес-процесів в інформаційно-комунікаційних системах на основі Інтернет технологій та застосунків.

Завданнями навчальної дисципліни є придбання навичок: аналізу потенційних загроз інформаційній безпеці та методів їх виявлення, оцінки та управління ефективного захисту інформації та інформаційних систем в сучасному цифровому середовищі, тестування на проникнення, відновлення після інцидентів, обробку подій безпеки та реагування на інциденти.

Предметом навчальної дисципліни є безпека інформаційно-комунікаційних систем.

Об’єктом вивчення дисципліни є технічні засоби, програмні продукти, процеси та методи, які використовуються для забезпечення безпеки інформації в системах, а також внутрішні та зовнішні загрози.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Здатність застосовувати знання у практичних ситуаціях. Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Здатність до пошуку, оброблення та аналізу інформації
Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.	Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 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.
Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	Здатність до пошуку, оброблення та аналізу інформації

	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.
Розробляти моделі загроз та порушника.	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	Здатність застосовувати знання у практичних ситуаціях. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	Здатність застосовувати знання у практичних ситуаціях. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність застосовувати методи та засоби криптографічного та технічного захисту

	інформації на об’єктах інформаційної діяльності. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	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 забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Застосунки мережевої безпеки

Тема 1. Сучасні загрози мережевої безпеки

1.1. Класи мереж

IP-адрес класу A/B/C/D/E та ідентифікатора мережі, ідентифікатора хоста.

1.2. Захист мереж

Концепції мережевої безпеки. Принципи система безпеки. Ключові елементи захищених мережних служб

1.3. Області мережевої безпеки

Багаторівневий захист: захист роутера, захист робочих станцій та захист окремих пристроїв.

1.4. Архітектура Cisco Security

Менеджер управління системою безпеки Cisco Security Manager (CSM); система моніторингу, аналізу та реагування системи безпеки Cisco Security (MARS); програмно-апаратне рішення для централізованого управління доступом Cisco Secure Access Control Server (ACS); платформа централізованого управління мережевою інфраструктурою Cisco IP Solution Center (ISC).

Тема 2. Забезпечення безпеки мережевих пристроїв

2.1. Захист граничного маршрутизатора

Протокол граничного шлюзу (BGP). Загальні порти, використовувані для BGP. Інструменти для використання BGP. Слабкі місця та уразливості BGP.

2.2. Призначення адміністративних ролей

Об'єкти-користувачі та їх атрибути доступу. Порядок створення та знищення об'єктів-користувачів відповідного типу.

2.3. Захист управління та звітності

Конфіденційність при обміні. Функціональні послуги безпеки "Реєстрація", “Ідентифікація та автентифікація" тощо.

2.4. Використання автоматичних функцій забезпечення безпеки

Захист за допомогою служби "Безпека у Windows".12:24

Тема 3. Автентифікація, авторизація та облік

3.1. Огляд AAA

Аутентифікація без AAA. Компоненти AAA (аутентифікація, авторизація, аудит). Режими аутентифікації. Авторизація. Аудит.

3.2. Конфігурування локальної аутентифікації AAA за допомогою інтерфейсу командного рядка (CLI)

Аутентифікація адміністративного доступу. RADIUS. TACACS +. Основні відмінності між RADIUS та TACACS +. Методи аутентифікації. Стандартний та іменований методи. Точне налаштування конфігурації аутентифікації.

3.3. Характеристики серверної аутентифікації AAA

Порівняння локальної та серверної аутентифікації AAA. Знайомство з системою управління захищеним доступом Cisco (Access Control System, ACS). Комунікаційні протоколи серверного AAA

3.4. Конфігурація серверної аутентифікації AAA за допомогою інтерфейсу командного рядка (CLI)

Процедура настройки серверної аутентифікації AAA за допомогою інтерфейсу командного рядка (CLI). Конфігурування використання серверів TACACS+ через CLI. Конфігурування використання серверів RADIUS через CLI. Конфігурування аутентифікації з використанням сервера AAA.

Тема 4. Впровадження технологій брандмауера

4.1. Список контроля доступу.

Налаштування стандартного і розширеного ACL-списків IPv4 з використанням інтерфейсу командного рядка (CLI). Короткі відомості про списки контролю доступу. Налаштування нумерованих і іменованих списків ACL. Застосування

ACL-списку. Редагування існуючих ACL-списків. Захист від спуфінга за допомогою ACL-списків. Пропуск необхідного трафіку через міжмережевий екран. Протидія зловмисному використанню протоколу ICMP. Нейтралізація експлойтів SNMP. Знайомство з ACL-списками IPv6

4.2. Технології між мережевого екрана.

Захист мереж за допомогою міжмережевого екрана. Визначення міжмережевого екрана. Переваги та обмеження міжмережевих екранів. Опис типів міжмережевих екранів. Переваги та обмеження брандмауера з фільтрацією пакетів. Міжмережеві екрани зі збереженням стану. Міжмережеві екрани нового покоління.

4.3. Зональні міжмережеві екрани.

Огляд зонального міжмережевого екрана (ZPF). Переваги ZPF. Дизайн ZPF. Принципи роботи ZPF. Дії ZPF. Конфігурування ZPF. Перевірка конфігурації ZPF.

Тема 5. Впровадження системи запобігання вторгнень

5.1. Технології IPS.

Характеристики систем IDS та IPS. Мережеві реалізації IPS. Cisco Switched Port Analyzer. Конфігурація Cisco SPAN з використанням системи виявлення вторгнень.

5.2. Сигнатури IPS.

Характеристики сигнатур IPS. Сигнали тривоги сигнатур IPS. Дії сигнатури IPS. Управління та моніторинг IPS. Глобальна кореляція IPS

5.3. Впровадження IPS.

Конфігурування Cisco IOS IPS за допомогою інтерфейсу командного рядка (CLI). Зміна сигнатур Cisco IOS IPS. Перевірка та моніторинг IPS.

Змістовий модуль 2. Мережева безпека

Тема 6. Забезпечення безпеки локальної мережі (LAN)

6.1. Безпека кінцевих пристроїв.

Знайомство з безпекою кінцевих пристроїв. Захист від шкідливого ПЗ. Захист електронної пошти та веб-трафіка. Контроль мережевого доступа.

6.2. Фактори забезпечення безпеки 2 рівня

Загрози безпеки 2 рівня. Атаки на таблиці CAM. Нейтралізація атаки на таблицю CAM. Нейтралізація атак на VLAN. Нейтралізація DHCP-атак. Нейтралізація ARP-атак. Нейтралізація атак спуфінга адрес. Протокол зв'язувального дерева. Нейтралізація STP-атак.

Тема 7. Криптографічні системи.

7.1. Захищені комунікації.

Аутентифікація, цілісність та конфіденційність. Складання шифротекста. Перестановочні шифри. Шифри заміни. Шифри One-Time Pad (Одноразовий блокнот). Зламування коду.

7.2. Криптологія.

Створення і злом секретних кодів. Криптоаналіз.

7.3. Криптографічні хеші.

Криптографічна хеш-функція. Властивості криптографічної хеш-функції. Відомі хеш-функції. Забезпечення цілісності за допомогою алгоритмів MD5, SHA-1 та SHA-2. Аутентифікація за допомогою алгоритму HMAC. Управління ключами. Характеристики управління ключами. Довжина в просторі ключів. Типи криптографічних ключів.

7.4. Шифрування.

Два класи алгоритмів шифрування. Симетричне та асиметричне шифрування. Симетричне блочне та потокове шифрування. Вибір алгоритму шифрування. Стандарт шифрування даних (DES). Використання 3DES. Огляд стандарту AES. Альтернативні алгоритми шифрування. Обмін ключами Діффі-Хеллмана.

7.5. Криптографія з відкритим ключем.

Порівняння симетричного і асиметричного шифрування. Алгоритми асиметричних ключів. Цифрові підписи. Інфраструктура відкритих ключів (PKI). Центри сертифікації. Сумісність різних постачальників PKI. Стандарти криптографії з відкритим ключем. Топології PKI. Цифрові сертифікати та CA.

Тема 8. Впровадження віртуальних приватних мереж (VPN).

8.1. Огляд мереж VPN.

Знайомство з мережами VPN. Мережі IPsec VPN 3-го рівня. Технології VPN. Два типи мереж VPN. Компоненти мереж VPN для віддаленого доступу. Компоненти мереж VPN між двома пунктами.

8.2. Знайомство з протоколом IPsec.

Технології IPsec. Протоколи IPsec. Internet Key Exchange.

8.3. Конфігурування IPsec VPN між двома пунктами (Site-to-Site)

Встановлення IPsec-з'єднання. Топологія IPsec VPN по схемі Site-to-Site. Політика ISAKMP. Політика IPsec. Криптокарта. IPsec VPN.

Тема 9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA)

9.1. Рішення ASA

Моделі міжмережевих екранів ASA. Розширення функціональність міжмережевого екрана ASA. Огляд міжмережевих екранів в дизайні мережі. Режими роботи міжмережевих екранів ASA. Вимоги до ліцензування ASA.

9.2. Конфігурація між мережевого екрана ASA

Базова конфігурація ASA. Рівні безпеки ASA. Сценарії розгортання ASA 5505. Знайомство з базовими налаштуваннями ASA. Налаштування сервісів та параметрів управління. Групи об'єктів. ACLS. Сервіси NAT на ASA. Сервісні політики в ASA.

Тема 10. Знайомство з ASDM

10.1. Знайомство з ASDM

Підготовка до роботи з ASDM. Запуск ASDM. Інформаційні панелі головної сторінки ASDM. Елементи сторінки ASDM. Розділи конфігурації та моніторингу ASDM. Меню майстрів ASDM. Налаштування сервісів і параметрів управління. Конфігурування розширених функцій ASDM.

10.2. VPN між двома пунктами (Site-to-Site)

Підтримка пристроєм ASA Site-to-Site VPN. VPN віддаленого доступу (Remote-Access). Порівняння IPsec і SSL. Захищений мобільний клієнт Cisco AnyConnect

Secure Mobility Client. Конфігурування SSL VPN без використання клієнта. Конфігурування SSL VPN з використанням клієнта AnyConnect.

Тема 11. Управління безпечної мережею

11.1. Техніки тестування безпеки мережі

Тестування та оцінювання безпеки мережі. Типи мережевих тестів. Інструменти тестування безпеки мережі.

11.2. Огляд політики безпеки

Життєвий цикл забезпечення мережевої безпеки. Політика безпеки. Аудиторія політики безпеки. Структура політики безпеки. Стандарти, інструкції та процедури. Ролі та обов'язки. Реагування на компрометацію системи безпеки.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2

Таблиця 2

Перелік лабораторних занять

Назва теми та / або завдання	Зміст
Тема 1, 2. Лабораторна робота 1.	Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.
Тема 3, 4. Лабораторна робота 2.	Захист маршрутизатора для адміністративного доступу.
Тема 5, 6. Лабораторна робота 3.	Захист адміністративного доступу за допомогою AAA і RADIUS.
Тема 7, 8. Лабораторна робота 4.	Налаштування зональних міжмережевих екранів.
Тема 9, 10, 11. Лабораторна робота 5.	Налаштування системи запобігання вторгнень (IPS).

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1. Завдання 1	Сучасні загрози мережевої безпеки.
Тема 2. Завдання 2.	Забезпечення безпеки мережевих пристроїв.
Тема 3. Завдання 3.	Автентифікація, авторизація та облік.
Тема 4. Завдання 4.	Впровадження технологій брандмауера.

Тема 5. Завдання 5.	Впровадження системи запобігання вторгнень.
Тема 6. Завдання 6.	Забезпечення безпеки локальної мережі (LAN).
Тема 7. Завдання 7.	Криптографічні системи захисту інформації.
Тема 8. Завдання 8.	Впровадження віртуальних приватних мереж (VPN).
Тема 9. Завдання 9.	Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).
Тема 10. Завдання 10.	Знайомство з ASDM.
Тема 11. Завдання 11.	Управління безпечною мережею.

Кількість годин лекційних та лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:
Словесні (лекції 1-10), проблемна лекція (Тема 11).
Наочні (демонстрація (Тема 1-11)).
Практичні (лабораторні роботи (Теми 1-10)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.
Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів: для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.
Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.
Семестровий контроль проводиться у формах диференційованого заліку або заліку.
Підсумкова оцінка за навчальною дисципліною визначається для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю.
Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:
Поточний контроль: індивідуальні завдання під час захисту лабораторних робіт (60 балів), дві письмові контрольні роботи (40 балів).
Семестровий контроль: Залік.

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсеєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с.
3. Інформаційна безпека держави: навчальний посібник / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус. - Харків : ТОВ «ДІСА ПЛЮС», 2018. – 359 с.
4. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-комунікаційних системах https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
5. Молчанов В. П. Технології розробки WEB-ресурсів [Електронний ресурс] : навч. посіб. / В. П. Молчанов, О. К. Пандорін ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (7,94 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 129 http://www.repository.hneu.edu.ua/handle/123456789/22466
6. Інформатика в сфері комунікацій [Електронний ресурс] : навч.-практ. посіб : у 3-х ч. Ч. 2 : Обробка та аналіз даних / С. Г. Удовенко, О. В. Тесленко, Н. О. Бринза [та ін.] ; за заг. ред. С. Г. Удовенка; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (14,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 249 с http://repository.hneu.edu.ua/handle/123456789/23347

Додаткова

7. Shmatko O. New method for assessing the risk of automated information systems information security based on fuzzy-multiple approach / O. Shmatko, N. Romaschenko. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020. – P. 93–104. http://repository.hneu.edu.ua/handle/123456789/24819
8. Milov O. Creation of a methodology for building security systems for multimedia information resources in social networks / O. Milov, S. Milevskyi, V. Aleksiyev. // Przetwarzanie, transmisja i bezpieczenstwo informacji. – Bielsko-Biala : Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsko-Bialej, 2020. - Vol. 12. - S. 185-192. http://repository.hneu.edu.ua/handle/123456789/24817
9. CNA 200-301 Official Cert Guide Library By Wendell Odom, Published Dec

31, 2019 by Cisco Press. Part of the Official Cert Guide series https://issuhub.com/view/index/33465
10. Synergy of building cybersecurity systems: monograph / Edited by S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://repository.hneu.edu.ua/handle/123456789/25623
11. Shmatko O. Information support for distributed teamwork knowledge management / O. Shmatko, M. Bilova. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– P. 169–192. http://repository.hneu.edu.ua/handle/123456789/24818

Інформаційні ресурси

12. EVE - віртуальне середовище в області мереж, безпеки та DevOps https://www.eve-ng.net/
11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “ Інженерія безпеки інформаційно-комунікаційних систем”
https://pns.hneu.edu.ua/enrol/index.php?id=10209