Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІНИХ СИСТЕМАХ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Другий (магістерський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*І рік підготовки, осінній семестр*
Обсяг дисципліни	*4 кредити*
Семестровий контроль/ контрольні заходи	*Екзамен, модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	

Київ 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна "*Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах*" передбачена освітньо-професійною програмою підготовки здобувачів вищої освіти *Безпека державних інформаційних ресурсів*, *ступеня вищої освіти магістр.* Є навчальною дисципліною циклу професійної підготовки та відноситься до нормативних освітніх компонентів.

Метою навчальної дисципліни "Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах" є формування у курсантів системи знань в області забезпечення кібербезпеки, а також застосування на практиці методів оцінки захищеності та захисту інформації. Особлива увага приділяється оцінці захищеності інформаційних систем та технологіям виявлення та протидії кібератакам на інформаційні системи.

Предметом навчальної дисципліни є системи виявлення вторгнень та системи захисту державних інформаційних ресурсі.

Основне завдання навчальної дисципліни "Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах" є формування наступних компетентностей:

КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2	Здатність проводити дослідження на відповідному рівні.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4	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.
КФ5	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.
КФ7	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.
КФ9	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.
КФ11	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.

Виконання програми навчальної дисципліни “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах” дозволяє досягти курсантами наступних результатів навчання:

РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення
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.
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики 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\абокібербезпеки в цілому.
РН21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН24	Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішне вирішення завдань навчальної дисципліни “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-

комунікаційних системах" базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр. Навчальна дисципліна забезпечує *"Кібернавчання", "Військове стажування",* а також виконання магістерської дисертації.

3. Зміст навчальної дисципліни

Семестровий (кредитний) модуль 1. Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаціних системах.
Тема 1. Виявлення та протидія локальним мережевим атакам.
Тема 2. Оцінка вразливостей систем електронних комунікацій.
Тема 3. Виявлення та протидія мережевим атакам в глобальних мережах.

4. Навчальні матеріали та ресурси

Основна література.

1. Rash, Michael. Linux firewalls: attack detection and response with iptables, psad, and fwsnort / Michael Rash.
2. Advanced Web Attacks and Exploitation, 2020, 445 p.
3. Nir Kshetri, Cybersecurity Management An Organizational and Strategic Approach, - University of Toronto Press 2021, Toronto Buffalo London – 429 p.
4. Badotra, Sumit, and Surya Narayan Panda. "SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking." Cluster Computing 24, 2021.

Додаткова література.

1. Eric C. Thompson, Lisle, Illinois. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. – USA, 2018, 184 p.
2. Mark Borrelli. Malware and computer security incidents handling guides. – 2013 Nova Science Publishers, Inc.
3. Sagar Ajay Rahalkar. Certified Ethical Hacker (CEH) Foundation Guide. – Library of Congress Control Number: 2016959970, 2016, 207 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальна дисципліна *"Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах"* вивчається курсантами на 1-ому курсі в осінньому семестрі.

Видами навчальних занять є лекції, практичні та самостійна робота.

Лекції є початковими заняттями в темах дисципліни. В них формуються головне завдання теми та викладаються основні напрямки його вирішення, вивчається конкретизований теоретичний матеріал.

На практичних заняттях курсанти закріплюють та поглиблюють знання, отримані на лекціях, з формуванням у них вмінь виконання окремих завдань з кібербезпеки інформаційних ресурсів, набувають практичних навичок моделюванні окремих елементів системи кібербезпеки державних інформаційних ресурсів, а також проводиться виконання практичного завдання.

Самостійна робота курсантів проводиться без керівництва викладача з метою самостійного закріплення та розширення знань.

В процесі вивчення дисципліни проводиться виховна робота зі курсантами. В процесі занять виховується наполегливість у переборенні труднощів, уміння

самостійно освоювати нові засоби та методи захисту інформації.

Поточний контроль знань та вмінь курсантів реалізується індивідуальним усним або груповим письмовим опитуванням на практичних заняттях.

Підсумковий контроль здійснюється у вигляді екзамену.

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практ. (семін.)	Лаборант. (комп.пр.)	СРК
Розділ 1. Технології виявлення загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах						
Тема 1.	**Виявлення та протидія локальним мережевим атакам**	**30**	**4**	**14**		**12**
Заняття 1/1	Аналіз та моніторинг мережевого трафіку. 1. Поняття “снiфінгу”. 2. Види моніторинг та аналізу трафіку. 3. Програмні та апаратні аналізатори протоколів. Основна література: [1-2].	**2,5**	2			0,5
Заняття 1/2	Мережевий аналізатор TCPdump. 1. Основні режими роботи мережевого інтерфейсу. 2. Ключі та фільтри. 3. Довідкова система. Основна література: [1-2].	**2,5**	2			0,5
Заняття 1/3	Мережевий аналізатор Wireshark. 1. Основні режими роботи мережевого інтерфейсу. 2. Ключі та фільтри. 3. Довідкова система. Основна література: [1-2].	**2,5**		2		0,5
Заняття 1/4	Атаки на протокол ARP. 1. Огляд протоколу ARP. 2. ARP spoofing. 3. MAC flooding. 4. Механізми захисту (DAI). Основна література: [1-2].	**2,5**		2		0,5
Заняття 1/5	Атаки на протокол DHCP. 1. Огляд протоколу DHCP. 2. DHCP spoofing та DHCP starvation. 3. Механізми захисту. Основна література: [1-4].	**3**		2		1
Заняття 1/6	Визначення вузлів мережі. 1. ICMP echo request. 2. Fping, Nmap. 3. TCP-ping та UDP-ping (hping3). 4. ARP-ping. Основна література: [1-2].	**3**		2		1

Заняття 1/7	Визначення топології мережі. 1. Ping Record Route. 2. Traceroute. 3. Додаткові засоби визначення маршрутів (NMAP, TRACEMAP, MRT). Основна література: [1-2].	**3**		2		1
Заняття 1/8	Ідентифікація статусу портів. 1. Статуси TCP-портів 2. Методи сканування UDP-портів. Основна література: [1-2].	**3**		2		1
Заняття 1/9	Ідентифікація статусу портів. 1. Методи прихованого сканування. 2. Модульна контрольна робота (частина 1). Основна література: [1-2].	**3**		2		1
Тема 2.	**Оцінка вразливостей систем електронних комунікацій**	**30**	**2**	**16**		**12**
Заняття 2/1	Мережеве сканування. 1. Огляд мережевого сканування. 2. Методології мережевого сканування. 3. Техніки та інструментарій. Основна література: [3-4].	**3**	2			0,5
Заняття 2/2	Ідентифікація мережевих сервісів та прикладних служб. 1. Аналіз банерів служб. 2. Дослідження засобами прикладних служб. 3. Евристичні методи. Основна література: [3-4].	**3**		2		0,5
Заняття 2/3	Ідентифікація операційних систем. 1. Активне дослідження стеку TCP/IP. 2. Пасивне дослідження стеку TCP/IP. 3. Евристичні методи. Основна література: [3-4].	**3**		2		0,5
Заняття 2/4	Система доменних імен. 1. Огляд системи DNS. 2. Основні загрози DNS. 3. Забезпечення безпеки. Основна література: [3-4].	**3**		2		0,5
Заняття 2/5	Безпека системи доменних імен. 1. Аналіз загроз безпеки системи доменних імен. 2. Вимоги і рекомендації до безпеки системи доменних імен. 3. DNS Security Extensions. Основна література: [3-4].	**3**		2		1
Заняття 2/6	Системи електронної поштової взаємодії. 1. Основні компоненти систем електронної пошти. 2. Протоколи електронної пошти. 3. Побудова листа електронної пошти. Основна література: [3-4].	**3,5**		2		1

Заняття 2/7	Аудит безпеки систем електронної поштової взаємодії. 1. Системний таймер. 2. Виконання задач в операційній системі. Основна література: [3-4].	**3,5**		2		1
Заняття 2/8	Сканування систем безпеки електронної поштової взаємодії. 1. Запис Mail Exchanger 2. Інфраструктура політики відправника 3. Технологія DomainKeys Identified Mail. Основна література: [3-4].	**3,5**		2		1
Заняття 2/9	Протокол забезпечення безпеки транспортного рівня SSL/TLS. 1. Загальні поняття протоколу SSL/TLS 2. Аналіз протоколу Record SSL/TLS 3. Порівняльний аналіз конструкцій AtE та EtA 4. Модульна контрольна робота (частина 2). Основна література: [3-4].	**3,5**		2		1
Тема 3.	**Виявлення та протидія мережевим атакам в глобальних мережах**	**30**	**2**	**16**		**12**
Заняття 3/1	Атаки відмови в обслуговуванні. 1. Концепції, ознаки. 2. Техніки DoS/DDoS атак. 3. Бонети. Основна література: [1-4].	**3,5**	2			0,5
Заняття 3/2	Атаки пост експлуатації. 1. Проникнення в систему з використанням атаки на стороні клієнта. 2. Локальне підвищення прав. 3. Отримання детальних відомостей про систему. Основна література: [1-4].	**3,5**		2		0,5
Заняття 3/3	Фрейворки Metasploite, Veil, Empire. 1. Призначення фреймворків. 2. Генерування корисного навантаження. 3. Методи обфускації. Основна література: [1-4].	**3,5**		2		0,5
Заняття 3/4	Виявлення та блокування атак пост експлуатації. 1. Виявлення аномалій мережевої взаємодії. 2. Аналіз локальних процесів. 3. Політики безпеки. Основна література: [1-4].	**3,5**		2		0,5
Заняття 3/5	Аутентифікація у ОС Windows. 1. Локальна аутентифікація. 2. Мережева аутентифікація. 3. Протокол Kerberos. Основна література: [1-4].	**3**		2		1

Заняття 3/6	Онлайн атаки на паролі. 1. Формування та зберігання паролів у різних системах інформаційних системах. 2. Типи атак на паролі. 3. Засоби атак на паролі. Основна література: [1-4].	**3**		2		1
Заняття 3/7	Офлайн атаки на паролі. 1. Перебір паролів. 2. Атаки з використанням радужних таблиць. Основна література: [1-4].	**3**		2		1
Заняття 3/8	Обхід систем мережевого екранування та виявлення вторгнень. 1. Концепція систем IDS/IPS, Firewall, HoneyPot. 2. Обхід IPS. 3. Обхід мережевих екранів. Основна література: [1-4].	**3**		2		1
Заняття 3/9	Сканери вразливостей. 1. Типи сканерів вразливостей. 2. Сканер XSpider. 3. Сканер Nessus. 4. Сканер OpenVAS. 5. Модульна контрольна робота (частина 3). Основна література: [1-4].	**3**		2		1
Разом за розділом 1		**90**	**8**	**46**		**36**
Екзамен		30				30
Всього годин		**120**	**8**	**46**		**66**

6. Самостійна робота здобувачів

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до екзамену.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
Тема 1. Технології виявлення загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах.		
1.	Програмні та апаратні аналізатори протоколів. Основні режими роботи мережевого інтерфейсу. MAC flooding. DHCP spoofing та DHCP starvation. Додаткові засоби визначення маршрутів (NMAP, TRACEMAP, MRT). Методи сканування UDP-портів. Основна література: [1-4]. Додаткова література: [1-3].	12
Тема 2. Оцінка вразливостей систем електронних комунікацій.		

2.	Методології мережевого сканування. Евристичні методи. Пасивне дослідження стеку TCP/IP. DNS Security Extensions. Побудова листа електронної пошти. Технологія DomainKeys Identified Mail. Порівняльний аналіз конструкцій AtE та EtA. Основна література: [1-4]. Додаткова література: [1-3].	12
Тема 3. Виявлення та протидія мережевим атакам в глобальних мережах .		
3.	Бонети. Отримання детальних відомостей про систему. Методи обфускації. Аналіз локальних процесів. Мережева аутентифікація. Засоби атак на паролі. Обхід мережевих екранів. Сканер OpenVAS Основна література: [1-4]. Додаткова література: [1-3].	12
4.	Підготовка до екзамену.	30
Всього годин		**66**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає систему вимог, які викладач ставить перед курсантами:

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені цим силабусом; у разі хвороби, несення служби в наряді або у виняткових випадках курсант може бути відсутнім на заняттях (з подальшим відпрацюванням пропущеного матеріалу самостійно або на консультаціях).

По прибутті на навчальні заняття курсанти повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника заняття; уважно слухати пояснення керівника заняття та відповіді одногрупників; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника навчального заняття; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної навчальної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання. В цьому випадку з курсантів вимагається обов'язково наявність справних відеокамери та мікрофону, які мають бути увімкнені на кожному дистанційному занятті. При проведення письмових контрольних заходів вимагається верифікація курсанта (фото з документом). Навчальна література навчальної дисципліни зазначена в розділі 4, є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання здобувачів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського.

Рейтинг з дисципліни складається з двох складових: стартової ($R_c = 60$ – призначена для оцінювання заходів поточного контролю впродовж семестру) та екзаменаційної ($R_e = 40$ – призначена для оцінювання на екзамені).

Рейтинг курсанта з освітнього компонента складається з балів, які він отримує за:

1) 15 виконаних та захищених практичних завдань, кожне з яких оцінюється у 3 бали;

2) модульну контрольну роботу (розділена на 3 частини роботи, кожна з яких оцінюється максимум в 3 балів);

3) 5 експрес-контролі (заняття № 1/7, 2/4, 2/7, 3/4, 3/7), кожне з яких оцінюється у 1 бал;

4) ведення конспекту лекції – 1 бал;

5) штрафні та заохочувальні бали (максимальна кількість рейтингових балів – не більше 6).

Система рейтингових (вагових) балів і критерії оцінювання

1. Виконання практичних завдань

Ваговий бал – 2. Максимальна кількість балів за всі завдання: 3б × 15 = 45 балів:

правильно і повністю виконані всі завдання, захист без запізнень – 3 б.

частково виконані завдання або наявні незначні помилки – 2 б.

завдання виконані з помилками або із запізненням – 1 б.

завдання не виконані – 0.

2. Контрольна робота

Ваговий бал – 3. Максимальна кількість балів за всі частини модульної контрольної роботи: 3б × 3 = 9 балів.

правильно і повністю виконані всі завдання – 3.

частково виконані завдання або наявні незначні помилки – 2.

завдання виконані з помилками – 1.

завдання не виконані – 0.

3. Експрес-контролі.

Ваговий бал – 1. Максимальна кількість балів: 1б × 5 = 5 балів.

правильно і повністю надані відповіді на питання – 1.

відповідь надано не повністю або не правильно – 0.

4. Ведення конспекту лекції

Ваговий бал – 1. Максимальна кількість балів: 1б × 1 = 1 бал.

конспект повний (в т.ч. питання, що виносяться на самопідготовку) – 1.

конспект не повний – 0.

Штрафні та заохочувальні бали за:

невчасно здані практичні завдання, пасивність на заняттях та несистематична самостійна робота протягом семестру -1… -6.

активність на заняттях та систематична самостійна робота протягом семестру, участь на олімпіадах та наукових конференціях +1…+ 6.

Календарна атестація курсантів проводиться за окремим розпорядженням КПІ ім. Ігоря Сікорського за результатами поточного рейтингу курсанта на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, курсант вважається атестованим.

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів складає R_c = 45+9+5+1 = 60 балів. Рейтингова оцінка з кредитного модуля формується як сума балів поточної успішності навчання – стартового рейтингу R_c та екзаменаційних балів R_e. Максимальна сума балів стартового рейтингу R_c складає 60. Необхідною умовою допуску до екзамену є те, що попередня рейтингова оцінка з кредитного модуля має бути не менше $0{,}6 \cdot R_c$ (36 балів), а також здані завдання всіх практичних занять і написані всі контрольні роботи.

Екзаменаційний білет містить 3 завдання: 2 теоретичних і 1 практичне.

Перше теоретичне питання з екзаменаційного білета оцінюється в 10 балів кожне, відповідно до системи оцінювання:

повна відповідь (не менше 90% потрібної інформації) – 10 балів;

достатньо повна відповідь (не менше 75% потрібної інформації або незначні неточності) – 8-9 балів;

неповна відповідь (не менше 60% потрібної інформації та деякі помилки) – 6-7 балів;

незадовільна відповідь – 0 балів.

Друге теоретичне питання з екзаменаційного білета оцінюється в 20 балів кожне, відповідно до системи оцінювання:

повна відповідь (не менше 90% потрібної інформації) – 20 балів;

достатньо повна відповідь (не менше 75% потрібної інформації або незначні неточності) – 15-19 балів;

неповна відповідь (не менше 60% потрібної інформації та деякі помилки) – 12-14 балів;

незадовільна відповідь – 0 балів.

Практичне завдання оцінюється у 20 балів:

повне безпомилкове розв’язування завдання – 18-19 балів;

достатньо повне розв’язування завдання – 15-17 балів;

завдання виконане з певними недоліками – 10-14 балів;

завдання не виконано – 0 балів.

Сума стартових балів та балів за екзаменаційну роботу переводиться до екзаменаційної оцінки згідно з таблицею:

Бали R=R_c + R_e	Оцінка
95-100	відмінно
85-94	дуже добре
75-84	добре
65-74	задовільно
60-64	достатньо
Менше 60	незадовільно
R_c< 36	не допущено

Заохочувальні та штрафні бали застосовуються вибірково та мають на меті підвищення мотивації курсантів до активної, відповідальної, системної роботи на заняттях протягом семестру.

9. Додаткова інформація з навчальної дисципліни

Орієнтовний перелік питань, що виносяться на семестровий контроль (екзамен):

1. Види моніторингу та аналізу трафіку
2. Програмні та апаратні аналізатори протоколів
3. Основні режими роботи мережевого інтерфейсу мережевого аналізатору TCPdump.
4. Ключі та фільтри мережевого аналізатору TCPdump.
5. Атаки на протокол ARP.
6. ARP spoofing
7. MAC flooding
8. Механізми захисту (DAI) від атаки на протокол ARP.
9. Атаки на протокол DHCP.
10. DHCP spoofing та DHCP starvation
11. Механізми захисту від атак на протокол DHCP
12. Визначення вузлів мережі: ICMP echo request, Fping, Nmap
13. Визначення вузлів мережі: TCP-ping та UDP-ping (hping3), ARP-ping
14. Визначення топології мережі.
15. Ідентифікація статусу портів.
16. Методи прихованого сканування.
17. Огляд мережевого сканування.
18. Методології мережевого сканування.
19. Техніки та інструментарій мережевого сканування.
20. Ідентифікація операційних систем.
21. Концепції, ознаки атаки відмови в обслуговуванні
22. Техніки DoS/DDoS атак
23. Ботнети
24. Виявлення аномалій мережевої взаємодії
25. Типи атак на паролі
26. Засоби атак на паролі
27. Атаки з використанням радужних таблиць.
28. Схема роботи сниффера

29. Ідентифікація мережевих сервісів
30. Аналіз банерів служб.
31. Дослідження засобами прикладних служб.
32. Евристичні методи дослідження мережевих сервісів.
33. Формат правил Snort.
34. Підходи аналізу шкідливого програмного забезпечення.
35. Техніка збору інформації “Login attempt”.
36. Класифікація кібератак на АС.
37. Принцип реалізації та приклади атак типу U2R.
38. Принцип реалізації та приклади атак типу R2L.
39. Принцип реалізації та приклади PROBE атак.
40. Принцип реалізації та приклади DDOS атак.
41. Механізми виявлення DDOS-атак
42. Створити правило Snort, що детектує скачування mp3-файлу, детектує доступ до забороненого сайту, для виявлення пакетів ICMP Echo Request, для виявлення обміну пакетами при обробці ping-запиту, для виявлення fin-сканування, для виявлення доступу до 3 різних сайтів, для виявлення вхідного запиту TCP-з’єднання, для виявлення спроби доступу до web-серверу, що перевіряє факт збігу IP-адрес, і відкидає пакет, якщо подібна атака має місце, тощо.
43. Виконати сканування типу “Login attempt” відносно трьох різних сервісів на віртуальній машині (рекомендовано Metasploitable).
44. Визначити служби, які працюють на кожному з відкритих портів на основі інформації, отриманої з банерів служб.