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

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 5

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*IV рік підготовки, осінній семестр*
Обсяг дисципліни	*5 кредитів*
Семестровий контроль / контрольні заходи	*Екзамен*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції: Олександр ШАПОВАЛ* *Практичні: Олександр ШАПОВАЛ*
Розміщення курсу	*Google Classroom*

Київ 2022

Програма навчальної дисципліни

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

Силабус освітнього компонента «Безпека інформаційних систем» складено відповідно до освітньої програми підготовки бакалаврів «Комп'ютерні системи і технології спеціального зв'язку» спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: (ЗК 1) здатність до абстрактного мислення, аналізу та синтезу; (ЗК 2) здатність застосовувати знання у практичних ситуаціях; (ЗК 3) знання та розуміння предметної області та розуміння професійної діяльності; (ЗК 6) здатність вчитися й оволодівати сучасними знаннями; (ЗК 8) здатність генерувати нові ідеї (креативність); (СК 3) здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем; (СК 9) здатність реалізувати багаторівневу обчислювальну модель на основі архітектури клієнт-сервер, включаючи бази даних, знань і сховища даних, виконувати розподілену обробку великих наборів даних на кластерах стандартних серверів для забезпечення обчислювальних потреб користувачів, у тому числі на хмарних сервісах; (СК 10) здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника; (СК 12) здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення; (СК 14) здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Предметом навчальної дисципліни є методи та засоби безпечної побудови, забезпечення функціонування, адміністрування та моніторингу інформаційних систем, які взаємодіють із глобальними комп’ютерними мережами (Інтернетом), як теоретична основа для об'єктів вивчення та діяльності, передбачених стандартом вищої освіти України щодо спеціальності 122 Комп'ютерні науки рівня бакалавр.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР 1) застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР 2) використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об’єктів інформатизації; (ПР 14) знати мережні технології, архітектури комп’ютерних мереж, мати практичні навички технології адміністрування комп’ютерних мереж та їх програмного забезпечення; (ПР 16) розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

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

Для успішного засвоєння дисципліни курсант повинен володіти освітніми компонентами «Технології розробки програмного забезпечення», «WEB-орієнтована розробка ПЗ», «Засоби і комплекси криптографічного захисту інформації» та «Технологічна практика». Компетенції, знання та уміння, одержані в процесі вивчення

освітнього компонента є необхідними для подальшого вивчення освітнього компоненту «Переддипломна практика (Військове стажування)».

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

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін:

Навчальні дисципліни, які забезпечуються цією навчальною дисципліною. Для успішного засвоєння учбового матеріалу дисципліни курсанти повинні мати підготовку в обсязі вищої школи за курсами “Фізика”, “Інформатика”, “Комп’ютерні мережі”, а також мати практичні навички роботи з комп’ютером. До дисциплін, вивчення яких безпосередньо спирається на навчальну дисципліну “Безпека інформаційних систем” відносяться: дисципліна “Проектування інформаційних систем”, експлуатаційна та переддипломна практики. Крім того, отримані під час проходження курсу знання можуть бути використані при виконанні кваліфікаційної роботи на випускових курсах.

4. Зміст навчальної дисципліни

Семестр 7

Семестровий (кредитний) модуль 1. Безпека інформаційних систем.

Розділ 1 Безпека інформаційних систем.

Тема 1. Еволюція і сучасний стан глобальних комп‘ютерних мереж.

Заняття: огляд мережевого обладнання рівня користувача та рівня провайдера (оператора).

Тема 2. Адресація та міжмережева маршрутизація в Інтернеті.

Заняття: використання адреси IP, маски, таблиці маршрутів, налаштування мережевого інтерфейсу. Таблиці RIB, політика маршрутизації, БД реєстрів маршрутизації.

Тема 3. Функціонування глобальних інформаційних сервісів в Інтернеті.

Заняття: Конфігурація DNS, файли зон, утиліти для роботи з резолвером. Поштові агенти, протоколи обміну повідомленнями e-mail. Практична взаємодія з HTTP-сервером. Формування запитів, аналіз відповідей, налаштування HTTP-сервера..

Тема 4. Попередження та виявлення інцидентів безпеки в глобальних комп‘ютерних мережах.

Заняття: конфігурування пакетних фільтрів та системи трансляції адрес. Застосування системи виявлення атак. Застосування сканерів вразливостей.

Тема 5. Безпечне налаштування та функціонування мережевих сервісів та глобальних інформаційних систем.

Заняття: безпечне конфігурування та захист DNS. Приклади застосування DNSSEC та TKIP. Безпечне конфігурування та захист SMTP-сервера. Безпечне конфігурування та захист HTTP-сервера.

5. Навчальні матеріали та ресурси

Основна література:

1. Ланде Д.В., Зубок В.Ю., Мохор В.В. Контури сучасних технологій побудови

глобальних інформаційних мереж: Методичний посібник з навчальної дисципліни “Сучасні технології побудови глобальних мереж” : Київ: ІСЗЗІ НТУУ “КПІ”. 2009. 195 с.

2. Програма мережної академії Cisco CCNA Exploration 5.0: електронний курс, 2016 р.

3. Зубок В.Ю., Корнейко О.В., Ланде Д.В. Безпека глобальних інформаційних систем та мереж : Київ: ІСЗЗІ НТУУ “КПІ”, 2010. 162 с.

4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: Київ: БХВ, 2009. 215 с.

5. T. Bates, E. Gerich. Representation of IP Routing Policies in a Routing Registry (ripe-81++): Електронний ресурс https://tools.ietf.org/html/rfc1786

6. Craig Hunt. TCP/IP Network Administration.Second Edition: O’Reilly, 2010. 417c.

Додаткова література:

1. Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman. Building Internet Firewalls. Second Edition: O’Reilly. 2000.

2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: ДСТСЗІ СБУ, Київ. 1999.

3. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: ДСТСЗІ СБУ. Київ, 1999.

4. Chris McNab, Network Security Assessment. 3nd Edition: O’Reilly, 2016. 494 p.

5. Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman. Building Internet Firewalls. Second Edition: O’Reilly, 2000.

6. Craig Hunt, TCP/IP Network Administration.Second Edition: O’Reilly, 1997.

7. НД ТЗІ 2.5-004-99, Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: ДСТСЗІ СБУ,Київ, 1999.

8. НД ТЗІ 2.5-005-99, Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: ДСТСЗІ СБУ, Київ, 1999.

Навчальний контент

6. Методика опанування навчальної дисципліни (освітнього компонента)

Методика опанування навчальної дисципліни (освітнього компонента) передбачає висвітлення інформації за розділами, темами) про всі навчальні заняття (лекції, практичні, семінарські, лабораторні) та надання рекомендацій щодо їх засвоєння (наприклад, у формі календарного плану чи деталізованого опису кожного заняття та запланованої роботи).

Самостійна робота курсанта містить інформацію про:

Види самостійної роботи (підготовка до аудиторних занять. Проведення розрахунків за первинними даними, отриманими на лабораторних заняттях, розв’язок задач, написання реферату, виконання розрахункової роботи, тощо).

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп`ютерний практикум)	СР
Розділ 1. *Безпека інформаційних систем*.						
Тема 1	**Еволюція і сучасний стан глобальних комп‘ютерних мереж**	**20**	**6**	**8**	**0**	**6**

Заняття 1/1	Основи безпеки в інформаційних системах. 1. Предмет та задачі кредитного модуля, Загальні звістки щодо кредитного модуля. 2. Основні складові інформаційної безпеки. 3. Важливість та складність проблеми інформаційної безпеки. Основна література: [1-4] Допоміжна література: [1]	**2**	2			
Заняття 1/2	Методи та засоби захисту інформації в ІС від несанкціонованого доступу. 1. Проблема несанкціонованого доступу. 2. Засоби обмеження фізичного доступу. 3. Засоби захисту від НСД в мережі. Основна література: [1-4] Допоміжна література: [1]	**3**	2			1
Заняття 1/3	Аудит і моніторинг безпеки. 1. Аудит системи безпеки. 2. Моніторінг системи безпеки. Основна література: [1-4] Допоміжна література: [1]	**3**		2		1
Заняття 1/4	Захист ІС від руйнуючих програм та вірусів. 1. Руйнуючи програми та їх класифікація 2. Методи виявлення та знешкодження вірусів 3. Методи захисту від комп'ютерних вірусів. Основна література: [1-4] Допоміжна література: [1]	**3**		2		1
Заняття 1/5	Безпека мережевих пристроїв 1. Безпечний доступ до пристроїв 2. Призначення адміністративних ролей 3. Моніторинг та управління пристроями. Основна література: [1-4] Допоміжна література: [1]	**3**	2			1
Заняття 1/6	Реалізація технологій запобігання вторгнення. 1. IPS технології 2. IPS підпис 3. Реалізація IPS. Основна література: [1-4] Допоміжна література: [1]	**3**		2		1

Заняття 1/7	Безпека локальної мережі 1. Безпека кінцевих пристроїв 2. Конфігурація безпеки другого рівня 3. Безпека безпровідних мереж, VoIP і SAN. Основна література: [1-4] Допоміжна література: [1]	**3**		2		1
Тема 2	**Адресація та міжмережева маршрутизація в Інтернеті**	**23**	**6**	**8**	**0**	**9**
Заняття 2/1	IP адресація. 1. Мережеві адреси IPv4. 2. Мережеві адреси IPv6. 3. Перевірка з'єднання. Основна література: [2,6] Допоміжна література: [1]	**3**	2			1
Заняття 2/2	Налаштування IP адрес. 1. Перетворення IPv4 адреси у двійкову форму. 2. Визначення IPv4 адреси. 3. Визначення IPv6 адреси. 4. Перевірка мережевого з'єднання. Основна література: [2,6] Допоміжна література: [1]	**3**	2			1
Заняття 2/3	Поділ мереж на підмережі. 1. Поділ IPv4 адреси на під мережі. 2. Адресні схеми. 3. Створення дизайну для IPv6 мережі. Основна література: [2,6] Допоміжна література: [1]	**3**	2			1
Заняття 2/4	Пристрій керування бездротовими точками доступу Aruba 7010. 1. Загальне конфігурування Aruba 7010. 2. Конфігурування аутентифікації на пристрої Aruba 7010. 3. Конфігурування шифрування на пристрої Aruba 7010. Основна література: [7]	**4**		2		2
Заняття 2/5	Бездротові точки доступу Aruba AP-345. 1. Загальне конфігурування Aruba AP-345. 2. Налаштування дводіапазонної роботи Aruba AP-345. 3. Налаштування зв'язку Aruba 7010 та AP-345 Основна література: [7]	**4**		2		2

Заняття 2/6	Прикладний рівень моделі TCP/IP. 1. Протоколи прикладного рівня. 2. Відомі протоколи і сервіси прикладного рівня. 3. Заголовок повідомлення. Основна література: [2,6] Допоміжна література: [1]	**3**		2		1
Заняття 2/7	Віртуальні локальні мережі VLAN. 1. Сегментація за допомогою VLAN. 2. Впровадження технології VLAN. 3.Захист VLAN та найкращі практики дизайну. Основна література: [2,6] Допоміжна література: [1]	**3**		2		1
Тема 3	**Функціонування глобальних інформаційних сервісів в Інтернеті**	**24**	**8**	**8**	**0**	**8**
Заняття 3/1	DNS. 1. Призначення DNS. 2. ПЗ серверів DNS. 3. Структура та принцип роботи DNS. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 3/2	Встановлення та базове налаштування bind. 1. Встановлення bind9 та перевірочних утиліт. 2. Структура файла зони. 3. Робота з утілітами. Основна література: [1-4] Допоміжна література: [1,5]	**3**		2		1
Заняття 3/3	Поштова система мережі Internet. 1. Принцип роботи поштової системи. 2. Протоколи поштової системи. 3. Серверне та клієнтське ПЗ. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 3/4	Встановлення та базове налаштування postfix. 1. Встановлення postfix з дисків. 2. Ручний запуск конфігуратора. 3. Перевірка роботи поштового сервера. Основна література: [1-4]	**3**		2		1

	Допоміжна література: [1,5]					
Заняття 3/5	Встановлення та базове налаштування exim. 1. Встановлення exim4 з дисків. 2. Встановлення клієнтського ПЗ. 3. Встановлення та налаштування серверного клієнтського ПЗ. Основна література: [1-4] Допоміжна література: [1,5]	**3**		2		1
Заняття 3/6	Протокол HTTP . 1. Принцип роботи протокола HTTP. 2. Формування http-запиту. 3. Структура http-відповіді. 4. Безпека http протоколу. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 3/7	Типи ПЗ HTTP серверів. 1. Internet Information Services. 2. Apache. 3. Nginx. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 3/8	Встановлення та базове налаштування Apache. 1. Встановлення apache2 та модулів. 2. Конфігурування apache2. 3. Формування ручного запиту. Основна література: [1-4] Допоміжна література: [1,5]	**3**		2		1
Тема 4	**Попередження та виявлення інцидентів безпеки в глобальних комп‘ютерних мережах**	**25**	**8**	**8**	**0**	**9**
Заняття 4/1	Порядок проходження пакетів через маршрутизатор. 1. Проходження пакетів від клієнта в глобальну мережу. 2. Проходження пакетів з глобальної мережі до клієнта. 3. Необхідність використання NAT. 4. Принципи роботи NAT. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1

Заняття 4/2	Пакетні фільтри. 1. Види та принципи роботи фільтрів. 2. Недоліки та переваги використання фільтрів. 3. Правила iptables. 4. Видача завдання на курсову роботу. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 4/3	Налаштування iptables. 1. Політики iptables. 2. Фільтри iptables. 3. Дії iptables. Основна література: [1-4] Допоміжна література: [1,5]	**4**		2		2
Заняття 4/4	Робота на платформі RangeForce. 1. Ознайомлення з інтерфейсом RangeForce. 2. Проходження сценаріїв платформи RangeForce. Основна література: [1-4] Допоміжна література: [1,5]	**6**		4		2
Заняття 4/5	Налаштування ланцюгів iptables. 1. Створення ланцюгів. 2. Застосування ланцюгів. Основна література: [1-4] Допоміжна література: [1.5]	**3**		2		1
Заняття 4/6	Системи виявлення вторгнень. 1. Open source системи. 2. Апаратні системи. 3. Журналювання дій. Основна література: [1-4] Допоміжна література: [1,5]	**3**	2			1
Заняття 4/7	Сканери вразливостей. 1. Типи сканерів вразливостей. 2. Небезпека використання сканерів вразливостей. Основна література: [1-4] Допоміжна література: [4-5]	**3**	2			1
Тема 5	**Безпечне налаштування та функціонування мережевих сервісів та глобальних інформаційних систем**	**28**	**8**	**8**	**0**	**12**

Заняття 5/1	Безпека серверного програмного забезпечення. 1. Загальні вимоги безпеки серверів. 2. Внутрішні програмні засоби безпеки . 3. Фізична безпека серверів. Основна література: [1-4] Допоміжна література: [4-5]	**3**	2			1
Заняття 5/2	Безпека DNS. 1. Фішингова атака. 2. Поняття DNSSEC. 3. Застосування DNSSEC. Основна література: [1-4] Допоміжна література: [4-5]	**3**	2			1
Заняття 5/3	Встановлення bind9 з DNSSEC. 1. Зміни налаштування для роботи DNSSEC. 2. Тестування роботи DNSSEC. 3. Встановлення плагінів DNSSEC для браузерів. Основна література: [1-4] Допоміжна література: [4-5]	**4**		2		2
Заняття 5/4	Безпека поштових систем. 1. Перехоплення електронного листа. 2. Протоколи POP3S та IMAPS. 3. Протокол SMTPS. Основна література: [1-4] Допоміжна література: [4-5]	**3**	2			1
Заняття 5/5	Встановлення та налаштування універсальної утиліти шифрування. 1. Встановлення stunnel4. 2. Налаштування stunnel4 для шифрування трафіку smtp. 3. Налаштування stunnel4 для шифрування трафіків pop3 та imap. Основна література: [1-4] Допоміжна література: [4-5]	**4**		2		2
Заняття 5/6	Встановлення та налаштування додаткових програм шифрування. 1. Встановлення та налаштування courier-pop3s. 2. Встановлення та налаштування courier-imaps. 3. Перевірка шифрування.	**4**		2		2

	Основна література: [1-4] Допоміжна література: [4-5]					
Заняття 5/7	Безпека web-серверів. 1. Необхідність шифрування трафіку HTTP. 2. Варіанти реалізації шифрування трафіку HTTP. Основна література: [1-4] Допоміжна література: [4-5]	**3**	2			1
Заняття 5/8	Налаштування HTTPS. 1. Налаштування stunnel4. 2. Налаштування власного шифрування серверу apache2. 3. Відключення .http. Основна література: [1-4] Допоміжна література: [4-5]	**4**		2		2
Разом за розділом 1		**120**	**36**	**40**	**0**	**44**
Екзамен		**30**	**0**	**0**	**0**	**30**
Всього годин		**150**	**36**	**40**	**0**	**74**

7. Самостійна робота курсанта

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
1	*Тема 1. Еволюція і сучасний стан глобальних комп'ютерних мереж.* *1. Основні напрямки несанкціонованого вторгнення.* *2. Виробники антивірусного ПЗ.* *3. Програмно-апаратні комплекси антивірусного захисту.* *4. ААА.* *5. Безпека систем віддаленого доступу.* *6. Типи електронних підписів.* *7. Виробники обладнання захисту периметру мережі.* *Основна література [1-4]*	6
2	*Тема 2. Адресація та міжмережева маршрутизація в Інтернеті.* *1. Перспективи розвитку IPv4* *2. Протокол ICMP* *3. Необхідність мережевої маски* *4. Недоліки VLSM* *5. Флаги IP-пакетів* *6. Стандарт IEEE 802.1Q* *Основна література [1-5]*	9
3	*Тема 3. Функціонування глобальних інформаційних сервісів в Інтернеті.* *1. Ресурсні записи DNS*	8

	2. Графічні утиліти DNS *3. Поштовий протокол Microsoft* *4. Postfixadmin* *5. Обмеження exim* *6. Протокол HTTPS* *7. Атака типу Man in the middle* *8. WEB-сервер Apple* *9. Модулі Apache* *Основна література [3-7]*	
4	*Тема 4. Попередження та виявлення інцидентів безпеки в глобальних комп'ютерних мережах.* *1. ACL* *2. Контекстні мережеві фільтри* *3. Firewall ufw* *4. Проксі-протокол Socks* *5. Графічні утиліти налаштування iptables* *6. Комерційні системи виявлення вторгнень.* *Основна література [1-5]*	9
5	*Тема 5. Безпечне налаштування та функціонування мережевих сервісів та глобальних інформаційних систем.* *1. Протипожежна безпека ЦОД* *2. Чому DNSSEC не знаходить масового застосування* *3. Альтернатива DNSSEC* *4. Безпека Microsoft Exchange Server* *5. Безпека Apache* *Основна література [1-7]*	12
6	*Підготовка до екзамену*	30
Всього годин		**74**

Політика та контроль

8. Політика навчальної дисципліни (освітнього компонента)

Правила захисту практичних робіт: в кожній практичній роботі має бути виконана практична частина та оформлений звіт, робота має бути захищена шляхом демонстрації практичної частини з поясненнями та відповіді на питання викладача.

Правила призначення заохочувальних та штрафних балів зазначені в РСО.

Політика дедлайнів та перескладань визначаються загальною політикою Інституту.

Політика академічної доброчесності: практичні роботи, що містять ознаки списування не приймаються і мають бути переробленими, а ті, що містять ознаки сторонньої допомоги при їх виконанні – також мають бути переробленими якщо курсант не надає вичерпних пояснень стосовно способу їх вирішення.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даного кредитного модуля можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальні матеріали та ресурси, зазначені у розділі 4 цього силабусу є відкритими, не містять відомостей з обмеженим доступом і можуть бути оприлюднені з використанням технологій дистанційного навчання, а сам силабус не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

9. 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 Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів (студентів) в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтинг курсанта з кредитного модуля “Безпека інформаційних систем” визначається балами за роботу на:

1) практичних заняттях;
2) екзамені.

При цьому враховуються заохочувальні (зі знаком “плюс”) та штрафні (зі знаком “мінус”) бали.

Система рейтингових (вагових) балів та критерії оцінювання

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

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою
Рейтингові бали, RDОцінка за університетською шкалою

Кількість балів	оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше ніж 60	Незадовільно

1. Рейтинг курсанта з навчальної дисципліни “Безпека інформаційних систем” визначається балами за:

3) 20 відповідей на практичних заняттях;
4) відповідь на екзамені.

При цьому враховуються заохочувальні (зі знаком “плюс”) та штрафні (зі знаком “мінус”) бали.

2. Критерії нарахування балів

2.1. Відповіді на практичних заняття оцінюються 3 балами кожне:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації) – 3 бали;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 2 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 1 бал;

– “незадовільно” – відповідь не відповідає вимогам до “задовільно” – 0 балів.

Тобто максимум 20*3 = 60 балів.

2.2. Відповідь на екзамені оцінюється 40 балами. Екзаменаційний білет складається з трьох запитань (два – теоретичних, одне – практичне).

Кожне теоретичне питання оцінюється 10 балами за такими критеріями:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 9…10 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними неточностями – 8 балів;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 6 - 7 балів;

– “незадовільно” – незадовільна відповідь – 0 балів.

Практичне питання оцінюється 20 балами за такими критеріями:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 18 … 20 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними неточностями – 15 … 17 балів;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 12 … 14 балів;

“незадовільно” – незадовільна відповідь – 0 балів.

2.3. Заохочувальні бали нараховуються за виконання творчих робіт у межах навчальної дисципліни (наприклад, підготовка рефератів та оглядів наукових праць, оригінальне виконання завдань на практичних і лабораторних заняттях).

Тобто максимум (+1)*6 = + 6 балів.

– штрафні бали нараховуються за несвоєчасне виконання завдань, що виносяться на практичні та лабораторні заняття.

Тобто максимум (–1)*6 = –6 балів.

$$RD = 100 = \sum_k r_K + \sum r_E + \sum r_Ш$$

3. Календарний контроль (атестація) проводиться згідно Графіка-календаря освітнього процесу ІСЗЗІ КПІ ім. Ігоря Сікорського на навчальний рік.

Умовою атестації є отримання не менше 50% від кількості балів, яку курсант може отримати на час її проведення.

4. Умовою допуску до екзамену є: виконання усіх завдань, що передбачені робочою програмою навчальної дисципліни на семестр з цієї навчальної дисципліни та отримання стартового рейтингу не менше 36 балів.

10. Додаткова інформація з навчальної дисципліни

Перелік питань, які виносяться на семестровий контроль

1. Засоби захисту від НСД в мережі.
2. Методи виявлення та знешкодження вірусів.
3. Загальні відомості за загрози інформаційній безпеці комп’ютеризованих систем.
4. Технологія брандмауер.
5. Руйнуючи програми та їх класифікація.
6. Технологія ААА.
7. Проблема несанкціонованого доступу.
8. Комплексний підхід щодо забезпечення інформаційної безпеки комп’ютеризованої системи.

9. Безпечний доступ до пристроїв.
10. Сучасні загрози мережевої безпеки.
11. Конфігурація безпеки другого рівня.
12. Локальна AAA аутентифікація.
13. Методи виявлення та знешкодження вірусів.
14. ACL.
15. Безпечний доступ до пристроїв.
16. Локальні, глобальні мережі та Internet.
17. Побудова простої мережі.
18. Порядок передавання даних у мережі.
19. Використання програми Wireshark для дослідження трафіку.
20. Використання команд ping та traceroute для дослідження Інтернет.
21. Протокол розв’язування адрес ARP.
22. Комутатори в локальних мережах.
23. Маршрутизатори в локальних мережах.
24. MAC адреси мережевого пристрою.
25. Огляд таблиці маршрутизації на комп’ютері.
26. Перетворення IPv4 адреси у двійкову форму.
27. Загрози мережевій безпеці.
28. Адресація IPv4.
29. Перетворення IPv4 адреси у двійкову форму.
30. Адреси IPv4 для різних цілей.
31. Мережі – розділення пристроїв на групи.
32. Архітектура мережі на канальному рівні.
33. Конфігурація комутатора та базові поняття комутації.
34. Загальні поняття VLAN.
35. Загальні поняття глобальних мереж.
36. Базові поняття ACL.
37. Стандартні IPv4 ACLs.
38. Розширені IPv4 ACL.
39. Технологія NAT.
40. Налаштування динамічної та статичної NAT.
41. Методи та засоби пошуку несправностей у мережах.

Розробник(и) робочої програми навчальної дисципліни (силабусу):