Університет КРОК | КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Назва курсу	**CSB022: Технології захисту інформації**
Викладач	Добришин Юрій Євгенович, к.т.н., доцент
Профайл викладача	https://www.krok.edu.ua/ua/pro-krok/spivrobitniki/dobrishin-yurij-evgenovich
Контактний телефон	(+38 044) 455-69-82
E-mail	dobr@krok.edu.ua
Консультації	Згідно з розкладом (online), MS Teams

1. Коротка анотація до курсу

Метою дисципліни є надання студентам теоретичних та практичних знань, навичок щодо застосування наявних технологій захисту інформації на базі сучасного програмного забезпечення інформаційно-телекомунікаційних систем, організації та практичної реалізації безпеки інформації у мережі передачі даних, а також адміністрування засобів захисту інформації та засобів аналізу захищеності автоматизованих систем.

2. Результати навчання

Програмні компетентності та результати навчання, компоненти яких формуються та розвиваються у курсі

Внесок дисципліни "Технології захисту інформації" в формування наступних програмних результатів навчання:

Програмний результат навчання	Результат навчання з дисципліни
ПР15 розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Студент може: ● встановлювати та налаштовувати на роботу спеціалізоване програмне забезпечення щодо захисту інформації; ● забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації; ● проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів; ● здійснювати операції щодо аналізу стану захищеності мережі; ● виконувати операції з адміністрування програмного забезпечення засобів захисту інформації, мережних екранів, програмних засобів аналізу захисту інформації та виявлення атак.

Передумовою формування результатів навчання з дисципліни є володіння здобувачем на достатньому рівні наступних компетентностей:

Загальні компетентності:

ЗК3 Знання та розуміння предметної області та розуміння професійної діяльності;

ЗК11 Здатність приймати обґрунтовані рішення.

ЗК13 Здатність діяти на основі етичних міркувань.

Спеціальні компетентності:

СК14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

3. Обсяг курсу

Вид заняття	150 годин / 5 кредитів ECTS		
	форма навчання		
	денна	заочна	дистанційна
лекції	28	-	-
практичні заняття	14	-	-
лабораторні роботи	14	-	-
самостійна робота	60	-	-
консультації	4	-	-
підсумковий контроль	30	-	-

4. Технічне обладнання і програмне забезпечення

Технічне обладнання:

- комп'ютер/ноутбук;
- серверне комп'ютерне обладнання (навчальні сервера);
- мережне обладнання навчального класу.

Програмне забезпечення:

- програмне забезпечення Oracle Virtual Box.- (https://www.virtualbox.org);
- програмне забезпечення MS Office 365.

5. Політики курсу

Студенти мають дотримуватись кодексу академічної доброчесності: https://www.krok.edu.ua/download/nakazi/2018-10-18_kodeks-akademichnoi-dobrochesnosti.pdf

6. Схема курсу

Тиждень / кіл-ть годин	**Тема**	**Форма діяльності**	**Завдання / кіл-ть годин**	**Термін виконання**
Тиждень #1/	Основні поняття і тенденції захисту інформації	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
10 годин	Налагодження безпеки комп'ютера з використанням групової політики операційної системи Windows	практичне заняття	Вирішення практичних завдань / 2	
	Налагодження безпеки комп'ютера з використанням групової політики	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #2/	Нормативні документи системи ТЗІ в Україні	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
10 годин	Виявлення вразливостей за допомогою Microsoft Baseline Security Analyzer. Налаштування локальної політики паролів.	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Резервне копіювання компонентів операційної системи Windows	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #3/	Програмні засоби захисту ОС Windows	лекція	Тестування / 2	1 тиждень

10 годин	Зміна MAC адреси операційної системи Windows	практичне заняття	Вирішення практичних завдань / 2	
	Налаштування ідентифікації та автентифікації користувачів операційної системи Windows.	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #4/	Комп'ютерні віруси, технології захисту від комп'ютерних вірусів	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
10 годин	Вразливості протоколу ARP	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Моніторинг трафіка ARP. Вразливості протоколу ARP.	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #5/	Проблемні питання безпеки комп'ютерних мереж	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
10 годин	Аналізатор протоколів локальної обчислювальної мережі	практичне заняття	Вирішення практичних завдань / 2	
	Налаштування локальної політики паролів.	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #6/	Захист протоколів стеку TCP/IP	лекція	Тестування / 2	1 тиждень
10 годин	Виявлення мережних аналізаторів за допомогою програмного забезпечення CAIN	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Поняття мережних аналізаторів та їх характеристика	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #7/	Безпека протоколів ICMP, DNS	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
10 годин	Вивчення атаки на функцію фрагментації	практичне заняття	Вирішення практичних завдань / 2	
	Основні види мережних атак.	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #8/	Захист інформації з використанням міжмережних екранів	лекція	Тестування / 2	1 тиждень
10 годин	Встановлення мережного екрану та його налаштування	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Налаштування мережного екрану операційної системи Windows.	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #9/	Віртуальні приватні мережі - VPN	лекція	Тестування / 2	1 тиждень
10 годин	Работа с программним обеспечением Internet Scanner	практичне заняття	Вирішення практичних завдань / 2	
	Моделі захисту. Захист пам'яті та шифрування даних	самостійна робота	Відповіді на контрольні запитання / 6	
Тиждень #10/	Безпека протоколу WWW	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
12 годин	Налаштування протоколу IPS за допомогою програмного забезпечення Windows	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Забезпечення захисту мережі за допомогою протоколів PPTP та L2TP.	самостійна робота	Відповіді на контрольні запитання / 8	
Тиждень #11/	Безпека прикладних протоколів Інтернету	лекція	Тестування / 2	1 тиждень
12 годин	Налаштування VPN	практичне заняття	Вирішення практичних завдань / 2	
	Використання паролів і механізмів контролю за доступом. Цифрові підписи, порядок використання	самостійна робота	Відповіді на контрольні запитання / 8	
Тиждень #12/	Безпека електронної пошти	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
12 годин	Забезпечення захисту трафіка мережі за допомогою протоколу SSH	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Основні нормативні документи, що регламентують порядок захисту інформації в інформаційно-телекомунікаційних системах	самостійна робота	Відповіді на контрольні запитання / 8	

Тиждень #13/	Система виявлення атак	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
12 годин	Перевірка мережі за допомогою програми NMAP	практичне заняття	Вирішення практичних завдань / 2	
	Технічні засоби захисту інформації	самостійна робота	Відповіді на контрольні запитання / 8	
Тиждень #14/	Засоби захисту UNIX-подібних систем (зокрема, Linux)	лекція	Викладання теоретичного матеріалу / 2	1 тиждень
12 годин	Перевірка механізму DNSSpoofing	лабораторна робота	Звіт з виконання лабораторної роботи / 2	
	Основні напрямки розвитку програмних засобів захисту інформації в інформаційно-телекомунікаційних системах.	самостійна робота	Відповіді на контрольні запитання / 8	

7. Система оцінювання та вимоги

Загальна система оцінювання курсу	Для оцінювання знань студентів використовується рейтингова 100-бальна шкала та чотирибальна шкала (відмінно, добре, задовільно, незадовільно).
Практичні заняття / лабораторні роботи	Здача вирішених практичних завдань і звітів з лабораторних робіт повинна здійснюватися відповідно до встановлених дедлайнів. Виконані завдання завантажуються студентом у відповідні модулі на платформі Moodle. Завдання може бути оцінено максимально для практичних робіт у 35 балів, для лабораторних - у 35 балів. Іспит оцінюється відповідно до якості і правильності виконаних завдань: 2 питання максимально по 15 балів за кожне за умови правильної і повної відповіді, максимально 30 балів.
Умови допуску до підсумкового контролю	**Виконання всіх лабораторних робіт є обов'язковою умовою для допуску до складання іспиту**

8. Рекомендована література до курсу

Базовий підручник

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем-К: Видавнича група BHV, 2009. С.608. URL: http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2015/03/Graivorovskyi_Novikov.pdf

Допоміжна література

1. Ю. А. Тарнавський. Технології захисту інформації: підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах». Київ : КПІ ім. Ігоря Сікорського. 2018. С.162. URL: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ. 2013. С.476. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf.
3. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. К.: Вид. Національної академії внутріш. справ. 2012. С.104. URL: https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf
4. Богуш В.М. та інші. Основи кіберпростору, кібербезпеки та кіберзахисту: навчальний посібник. К.: Видавництво Ліра-К, 2020.

Онлайн-ресурси

1. Казарин О. В. Безопасность программного обеспечения компьютерных систем. URL: http://citforum.ru/security/articles/kazarin
2. Федотов Н. Н. Защита информации (Учебный курс). URL: http://www.college.ru/UDP/texts/index.html
3. Завгородний В.И. Комплексная защита информации в компьютерных системах. URL: http://sumi.ustu/discip/bis/Zavgorodnii/index.html
4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. М.: Академический проект, Фонд «Мир». 2003. С. 640. URL: http://sumi.ustu/discip/bis/books/ib.djvu
5. Скляров Д. Искусство защиты и взлома информации. URL: http://sumi.ustu/discip/bis/books/iz.djvu

До уваги студентів: усі навчально-методичні матеріали (презентації лекцій, тренувальні тести, тренувальні практичні завдання, завдання тощо) подані в Moodle за посиланням https://dist1.krok.edu.ua/course/view.php?id=11