

## **Антикризовий Центр кібернетичного захисту бізнесу при ТПП України пропонує семінари та практикуми з питань кібернетичної безпеки для малого та середнього бізнесу**

- 1. Технології побудови комплексних систем захисту інформаційних ресурсів організацій та установ згідно вітчизняних вимог та стандартів. Практичні рекомендації.**

Мета курсу – навчання слухачів методологічним (нормативно-правовими, організаційними та технічними) основам організації *комплексної системи захисту інформації (КСЗИ)* на підприємствах і установах, а також навчання широкому колу практичних аспектів діяльності по розробці, впровадженню, забезпеченню функціонування та контролю ефективності процесів КСЗИ згідно вітчизняних вимог та стандартів.

- 2. Технології побудови системи менеджменту інформаційної безпеки згідно міжнародних вимог та стандартів серії ISO. Практичні рекомендації.**

Мета курсу – навчання слухачів методологічним та практичним основам організації *системи менеджменту інформаційної безпеки* на підприємствах та установах з різними формами власності.

- 3. Технології побудови системи менеджменту кібернетичної безпеки згідно міжнародних вимог та стандартів ISO / IEC 27032:2012 та ISO/IEC 15408. Практичні рекомендації.**

Мета курсу – навчання слухачів методологічним та практичним основам організації *системи кібернетичної безпеки* на підприємствах, організаціях та установах згідно стандарту *ISO / IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Наставни щодо забезпечення кібербезпеки»* розроблений підкомітетом SC 27 «Інформаційні методи забезпечення безпеки» технічного комітету ISO/TC «Інформаційні технології».

- 4. Технології побудови систем кіберзахисту інформаційних ресурсів на базі обладнання Cisco.**

Офіційний Курс “Cybersecurity Essentials” Cisco Academy Connection.

Мета курсу – навчання слухачів методологічним та практичним основам організації *системи кібернетичної безпеки* на підприємствах, організаціях та установах на базі обладнання Cisco.

- 5. Офіційний Курс “CCNA R&S”.**

Курс побудований із 4-х частин. В основі курсу лежить вивчення технологій мереж та поглиблена теорія у галузі протоколів (LAN,WAN), розглянуті основні засоби захисту мереж на базі комунікаційного обладнання.

*Перша частина* - «Введення в мережеві технології - маршрутизація та комутація» присвячена вивченню основ побудови корпоративних мереж

*Друга частина* - «Основи маршрутизації та комутації». У рамках другої частини окремо розглянуті питання захисту інформаційних ресурсів від несанкціонованого вторгнення та кібер загроз.

*Третя частина* - «Маршрутизація и комутація. Масштабування мереж»

*Четверта частина* - «Маршрутизація и комутація. Об'єднання мереж»

Кожна частина курсу розрахована на 70 годин навчальних занять

*При успішному проходженні курсу слухачі отримують офіційний Сертифікат Cisco Academy Connection*

## **6. Технології адміністрування та захисту інформаційних ресурсів в інформаційно-комунікаційних системах та мережах.**

Мета курсу - підготовка фахівців з інформаційних технологій для виконання обов'язків посадових осіб служби захисту інформації (кібернетичного захисту) в автоматизованих системах, зокрема адміністраторів безпеки інформаційно-комунікаційних систем і мереж.

## **7. Організація комплексної безпеки об'єктів інформаційної діяльності.**

Мета курсу - підготовка фахівців з інформаційних технологій для виконання обов'язків посадових осіб Служби захисту інформації в автоматизованих системах.

## **8. Інформаційна безпека. Безпека програмного забезпечення комп'ютерних мереж (мережеві атаки) та розслідування кіберзлочинів. Правові приклади і вирішення розслідування інцидентів кібербезпеки**

Мета курсу – надання основних понять та принципів сучасних технологій з захисту цифрової інформації та розслідування кіберзлочинів. Створити умови для обміну досвідом фахівців, експертів, правознавців для професійного зростання слухачів та впровадження отриманих знань на практиці при розслідуванні кіберзлочинів.

Для кого призначений:

Курс розрахований на фахівців в області інформаційних технологій, фахівців в області безпеки операційних систем і прикладного програмного забезпечення, керівників відділів з інформаційної безпеки, керівників підприємств, юридичним відділам підприємств а також адвокатам працюючих з цифровими ІТ технологіями, а також проведення розслідувань та зборів доказів (комп'ютерна експертиза) по комп'ютерним інцидентам.

## **9. Інформаційна безпека. Аудит інформаційної безпеки підприємства. Юридичне оформлення та впровадження корпоративних стандартів безпеки.**

Мета курсу - надання основних понять та принципів сучасних технологій з захисту цифрової інформації та проведення аудиту інформаційної безпеки інфраструктури підприємств. Створення умов для обміну досвідом фахівців, експертів, юристів для професійного зростання та впровадження отриманих знань в практику забезпечення впевненості цілісності інформаційної безпеки підприємств.

Для кого призначений:

Курс розрахований на фахівців з комп'ютерних мереж, системним інженерам, керівникам ІТ відділів і підрозділів, керівників підприємств які хочуть перейти на міжнародні стандарти інформаційної безпеки серії ISO 27001, ISO 27002. Фахівців бажаючих освоїти основні напрямки вразливості програмного забезпечення та ознайомиться з механізмами його технічної і юридичного захисту. Фахівців з юридичних відділів компаній, експертам з інформаційної безпеки.

## **10. Інформаційна безпека. Створення та впровадження корпоративних стандартів безпеки на підприємстві. Основні засади впровадження стандартів серії ISO 27001. Юридичні практики та документальне оформлення процедур.**

Мета курсу - надання основних понять та принципів сучасних технологій з захисту цифрової інформації та впровадження корпоративних стандартів безпеки. Надати основні поняття та принципи впровадження стандартів інформаційної безпеки. Створити умови для обміну досвідом фахівців, експертів, юристів для професійного зростання та практичного застосування отриманих знань при впровадження стандартів інформаційної безпеки підприємств.

Для кого призначений:

Курс розрахований на фахівців з комп'ютерних мереж, системним інженерам, керівникам ІТ відділів, експертам бажаючим освоїти основні процедури аудиту інформаційної безпеки і впровадження систем менеджменту управління інформаційної безпеки. Керівників відділів і підрозділів, керівників підприємств які хочуть перейти на міжнародні стандарти інформаційної безпеки серії ISO 27001. Фахівців з юридичних відділів компаній, експертам з інформаційної безпеки.

## **11. Загальні засади кібергігієни.**

Мета курсу - надання основних понять та принципів сучасних технологій з захисту цифрової інформації та загальних правил поведінки в мережі Інтернет. Базові вимоги до користувачів. Базові рекомендації щодо безпечного користування програмними засобами.

Для кого призначений:

Пересічні користувачі, початковий рівень знань.

## **12. Захист критичних об'єктів бізнесу.**

**Мета курсу - надання основних понять щодо виявлення критичних процесів та об'єктів. Рекомендації щодо захисту. Базові рекомендації щодо технологій.**

**Для кого призначений:  
Власники бізнесу, користувачі.**

## **13. Основні технології захисту інформації в корпоративних мережах.**

**Для кого призначений:  
Власники бізнесу, виконавчі директори, директори.**

**Контактні особи: Анатолій Андрієнко, [aaa-zed@ucci.org.ua](mailto:aaa-zed@ucci.org.ua), 044 584 2819  
Анатолій Клікіч, 050 469 5282**