чих утиліт для кросбраузерного тестування Web-застосувань; аналіз обраних утиліт по раніше зазначеним критеріям; аналіз отриманих результатів.

47. БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ

к.ф-м.н. доц. Минко П.Є., Мельников О.О., ХНУРЕ, Харків

В доповіді здійснено аналіз сучасних засобів забезпечення безпеки хмарних технологій. За допомогою хмарних обчислень, підприємства і установи можуть отримати як послугу на вимогу усе від інфраструктури до програмного забезпечення. Провідні аналітичні компанії фіксують тенденції швидкого темпу росту витрат на cloud computing, а також на ринок супутніх сервісів, центрів обробки даних (ЦОД) і трафіку даних в таких системах. При цьому повинні ретельно дотримуватися вимоги технічних регламентів по захисту даних. Хмарна безпека повинна базуватися на комплексному підході, що поєднує шифровану передачу даних і надійність ЦОД, спроектованих з необхідною надмірністю. Ще одним важливим аспектом хмарної безпеки є передача даних між обладнанням користувача і ЦОД: усі дані мають бути зашифровані, а для роботи критично важливих для бізнесу застосувань мають бути гарантовані задовільні характеристики. Сучасні методи забезпечення хмарної безпеки здійснюють перевірку доступності застосувань і даних в аспекті безпеки: індивідуальні системи мають бути резервованими, а центри обробки даних повинні мати функцію зеркалювання.

48. СУЧАСНІ ВИКЛИКИ КІБЕРЗЛОЧИННОСТІ

к.н.д.у. Онищенко Ю.М., к.т.н. доц. Гнусов Ю.В., ХНУВС, Харків

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються злочини, що отримали назву «кіберзлочини». З поширенням використання інформаційних технологій в сфері управління, технологічних процесів зростає їх вразливість щодо вчинення правопорушень з використанням засобів комп'ютерної техніки. Таким чином, об'єкти енергетичного забезпечення, транспортні системи, фінансові і банківські структури, військові відомства та правоохоронні органи, торгівельні, медичні й наукові установи – усі, хто використовує всесвітню мережу Інтернет, є потенційними жертвами комп'ютерної злочинності, зокрема кібертероризму.

49. ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ НАВЧАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ В ЗАДАЧІ ПРОГНОЗУВАННЯ

д.т.н. проф. Руденко О.Г., Романюк О.С., ХНЕУ, ХНУРЕ, Харків

Перевагою штучних нейронних мереж (ШНМ) в задачах прогнозування є їх висока ефективність при моделюванні нелінійних залежностей, можливість роботи з зашумленими та неповними даними, їх здібність до навчання і адаптації до зовнішніх умов, що змінюються. Крім того, вважається, що нейромережеві методи дозволяють збільшити глибину прогнозу за рахунок виявлення прихованих закономірностей взаємозв'язків процесу, що досліджується. При використанні ШНМ виникають задачі вибору структури мережі та її навчання (визначення її параметрів). Задача суттєво ускладнюється при вирішенні її в нестаціонарних умовах, що призводить до підвищення вимог до алгоритмів навчання. В доповіді досліджуються властивості існуючих алгоритмів навчання та пропонуються різні їх модифікації, метою яких є прискорення процесу навчання мережі з одночасним зменшенням запізнення оцінювання та можливого зміщення