Inteligentne systemy przeciw atakom sieciowym

wykład

Przedmiot

Joanna Kołodziejczyk

2016

Program przedmiotu

Dwie formy zajęć:

1. Wykład - (Stacjonarne 15h) (Niestacjonarne 10h)
2. Projekt - obowiązkowy (Stacjonarne 30h) (Niestacjonarne 20h)

Elementami kształcenia w zakresie wiedzy

- EKW1: ma elementarną wiedzę z zakresu podstaw informatyki obejmującą metody inteligentnej analizy danych przesyłanych w sieci (K_W04 (ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych, K_W11 ma szczegółową wiedzę z zakresu projektowania oraz funkcjonowania technologii internetowych))
- EKW3: zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony zasobów sieciowych (K_W16 ma szczegółową wiedzę w zakresie bezpieczeństwa i higieny pracy)

Elementami kształcenia w zakresie umiejętności

- EKU1: potrafi rozpoznać zagrożenia zasobów, potrafi pozyskać bieżącą wiadomości na temat bezpieczeństwa (K_U07 (potrafi wykorzystać poznane metody i modele matematyczne, a także symulacje komputerowe do analiz, projektowania i oceny baz danych, aplikacji internetowych, systemów i sieci komputerowych) K_U08 (potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe))
- EKU2: potrafi wykorzystywać inteligentne metody, do analizy prób włamań i wyciągnąć wnioski (K_U13 (potrafi zaprojektować proces testowania oprogramowania oraz — w przypadku wykrycia błędów — przeprowadzić ich diagnozę i wyciągnąć wnioski), K_U19 (potrafi konfigurować urządzenia komunikacyjne w lokalnych (przewodowych i radiowych) sieciach teleinformatycznych, przestrzegając zasady bezpieczeństwa))

Elementami kształcenia w zakresie kompetencji społecznych

- EKK1: prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu inżyniera odpowiedzialnego za bezpieczeństwo sieci komputerowych (K_K05 prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu inżyniera informatyka)
- EKK2: potrafi przewidywać i działać w sposób umożliwiający uprzedzające eliminowanie zagrożeń sieciowych (K_K06 - potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy)

Program wykładów

1. Problemy bezpieczeństwa sieci a sztuczna inteligencja (Stacjonarne 3h) (Niestacjonarne 2h)
2. Sztuczne sieci neuronowe jako klasyfikator (Stacjonarne 3h) (Niestacjonarne 2h)
3. Nive Bayes w systemach IDS (Stacjonarne 3h) (Niestacjonarne 2h)
4. Drzewa decyzyjne w systemach IDS (Stacjonarne 3h) (Niestacjonarne 2h)
5. Inne metody sztucznej inteligencji (Stacjonarne 2h) (Niestacjonarne 1h)
6. Zaliczenie (1h)

Program projektu

1. WEKA — Instalacja, obsługa, możliwości, test na prostym zbiorze.
   (Stacjonarne 4h) (Niestacjonarne 4h)
2. Dane wejściowe. Zbiory zawierające dane z ataków sieciowych. Analiza danych tzw. preprocessing z użyciem WEKA.
   (Stacjonarne 3h) (Niestacjonarne 2h)
3. Zastosowanie sztucznych sieci neuronowych jako klasyfikatora. Wykorzystanie WEKA do danych KDD'99. Analiza otrzymanych wyników.
   (Stacjonarne 5h) (Niestacjonarne 4h)
4. Zastosowanie naiwnego klasyfikatora Bayesa jako klasyfikatora.
   (Stacjonarne 5h) (Niestacjonarne 3h)
5. Zastosowanie algorytmu kNN do identyfikacji włamań.
   (Stacjonarne 5h) (Niestacjonarne 3h)
6. Zastosowanie drzew decyzyjnych do tworzenia reguł wykrywających atak.
   (Stacjonarne 4h) (Niestacjonarne 2h)
7. Dostępne narzędzia do monitorowania bezpieczeństwa w sieciach - przegląd.
   (Stacjonarne 4h) (Niestacjonarne 2h)

Metody weryfikacji - projekt

Ocena:

1. P = Praca na zajęciach oceniana w skali (0-1)
2. Z = Zadania, testy do wykonania na zajęciach (0-1)
3. H = Zadania domowe, sprawozdania z wykonanych prac (0-1)

Kryteria oceny - projekt

$$\text{Punktacja końcowa} = 10\% * \frac{P}{maxP} + 30\% \frac{Z}{maxZ} + 60\% \frac{H}{maxH},$$

gdzie max — maksymalna liczba punktów do zdobycia (zależy od liczby zajęć i zadań)

np. $P = 0{,}90 + 0{,}5 + 1 + 1 + 1 = 4{,}4$; $\text{maxP} = 5$
$Z = 1 + 0{,}6 + 0{,}4 + 0{,}8 + 1 + 1 = 4{,}8$; $\text{maxZ} = 6$
$H = 1 + 0 + 0 + 0{,}7 = 1{,}7$; $\text{maxH} = 4$

$$\text{Punktacja końcowa} = 10\% * \frac{4{,}4}{5} + 30\% \frac{4{,}8}{6} + 60\% \frac{1{,}7}{4} = 0,583$$

Tabela przeliczania - projekt

Punktacja końcowa	Ocena końcowa
$x < 0,5$	2
$0,5 <= x < 0,6$	3
$0,6 <= x < 0,7$	3,5
$0,7 <= x < 0,8$	4
$0,8 <= x < 0,9$	4,5
$x >= 0,9$	5

Metody weryfikacji - wykład

Test z tematyki przedmiotu na ostatnich zajęciach. Test wyboru. Wybór jednej poprawnej odpowiedzi z czterech możliwości. Czas 1h.

Punktacja test	Ocena test
$x < 0,5$	2
$0,5 <= x < 0,6$	3
$0,6 <= x < 0,7$	3,5
$0,7 <= x < 0,8$	4
$0,8 <= x < 0,9$	4,5
$x >= 0,9$	5

Ocena - wykład

Ocena końcowa = 60% oceny z proj. +40%test
Wszystkie formy muszą mieć pozytywną ocenę na zaliczenie np. nie można mieć z testu ndst i zaliczyć.

np.
projekt = 4
test = 3

ocena końcowa = 2,4 + 1,2 = 3,6

Tabela przeliczania - wykład

Ocena pośrednia	Ocena końcowa
$x < 3$	2
$3 <= x < 3,25$	3
$3,25 <= x < 3,75$	3,5
$3,75 <= x < 4,25$	4
$4,25 <= x < 4,75$	4,5
$x >= 4,75$	5