KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo w systemach przechowywania danych

Przedmiot

Kierunek studiów
informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
30	15	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Tomasz Bilski
tomasz.bilski@put.poznan.pl
tel: 61 665 35 54
Wydział Informatyki i Telekomunikacji
Instytut Informatyki

Odpowiedzialny za przedmiot/wykładowca:
mgr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl
tel: 61 665 39 92
Wydział Informatyki i Telekomunikacji
Instytut Informatyki

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć: ogólną wiedzę na temat architektury systemów komputerowych, systemów operacyjnych, sieci komputerowych (w tym protokołów komunikacyjnych), baz danych.

Cel przedmiotu

Przekazanie studentom wiedzy i umiejętności dotyczących bezpieczeństwa w systemach długotrwałego przechowywania danych, z uwzględnieniem różnych rodzajów nośników danych (dysków i taśm magnetycznych, pamięci optycznej, pamięci półprzewodnikowej (flash) oraz różnych architektur systemów przechowywania (w tym: SAN, cloud storage, architektury zwirtualizowane).

Przedmiotowe efekty uczenia się

Wiedza

1. student ma wiedzę na temat różnych metod technologii przechowywania danych: magnetycznych, optycznych, półprzewodnikowych,

2. student ma wiedzę na temat różnych modeli i architektur systemów przechowywania danych, z uwzględnieniem protokołów komunikacyjnych (w tym FC, iSCSI), architektur zwirtualizowanych, sieciowych (NAS, SAN, cloud storage)

3. student ma wiedzę na temat podatności i zagrożeń charakterystycznych dla systemów przechowywania danych

4. student ma wiedzę na temat metod, narzędzi i zasad ochrony dotyczących systemów przechowywania danych

Umiejętności

1. student potrafi opracować założenia, koncepcję i projekt systemu przechowywania danych z uwzględnieniem rozwiązań bazujących na sieciach komputerowych

2. student potrafi dokonać analizy budowy i funkcjonowania systemu przechowywania danych, z uwzględnieniem poziomu bezpieczeństwa

3. student potrafi zapewnić wysoki poziom bezpieczeństwa przechowywania danych

Kompetencje społeczne

1. student rozumie, że posługiwanie się narzędziami informatycznymi musi gwarantować wysoki poziom bezpieczeństwa przechowywanych danych

2. student rozumie, że konieczne jest aktualizowanie wiedzy i umiejętności z zakresu konkretnych narzędzi i systemów.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład

Kolokwium (45 minut) z pytaniami otwartymi. Kolokwium jest przeprowadzane na ostatnich zajęciach w semestrze. W celu uzyskania oceny pozytywnej trzeba otrzymać ponad 50% wszystkich możliwych do zdobycia punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania są przekazywane studentom na początku semestru.

Laboratoria

Umiejętności nabyte w ramach zajęć praktycznych weryfikowane są na bieżąco podczas zajęć (przy omawianiu kolejnych etapów i części projektu) oraz przez dokonanie końcowej oceny projektu i jego dokumentacji przez prowadzącego zajęcia.

Treści programowe

Wykład

1. Wprowadzenie – klasyfikacja i parametry (pojemność, BER, parametry wydajnościowe, czas życia) nośników danych (flash, magnetyczne, optyczne), organizacja logiczna (formatowanie, sektory uszkodzone, partycje, FAT, NTFS, HPFS).

2. Standardy magistral pamięci zewnętrznych (ATA, SATA, SCSI, SAS, FC, NVMe, Infiniband). Protokoły komunikacyjne dla sieciowych systemów przechowywania: iSCSI, FCIP, IFCP.

3. Magnetyczne nośniki danych, zasada rejestracji magnetycznej, organizacja danych. Dyski magnetyczne. Pamięci taśmowe (zapis helikalny, liniowy), standardy (QIC, DLT, SDLT, LTO).

4. Optyczne nośniki danych, dyski optyczne (technologia, kodowanie, budowa, organizacja danych), standardy (CD, DVD, Blu-ray).

5. Półprzewodnikowe nośniki danych (flash, SSD).

6. Podatności i zagrożenia charakterystyczne dla różnych rodzajów nośników i systemów przechowywania danych. Ogólna charakterystyka narzędzi, metod i zasad ochrony.

7. Kopie zapasowe (backup). Modele i strategie systemów kopii zapasowych, serwery archiwizujące, systemy hierarchicznego składowania i zarządzania danymi HSM (Hierarchical Storage Management), ILM, deduplikacja.

8. Wirtualizacja systemów przechowywania danych, pamięci masowe w sieciach komputerowych (NAS, SAN, VSAN). IP storage. Przechowywanie danych w chmurach: modele (w tym obiektowy model przechowywania danych), przykłady (w tym: Amazon Simple Cloud Storage Service). Bezpieczeństwo w systemach cloud storage.

9. Trwałość i niezawodność nośników oraz systemów przechowywania. Miary niezawodności (w tym: MTBF, BER, RTO, RPO). Nieodwracalne niszczenie danych.

10. Zastosowania technik kryptograficznych w systemach przechowywania danych (metody szyfrowania danych na dyskach twardych, szyfrowanie danych w chmurach, szyfrowanie pamięci typu pendrive).

11. Aktualne problemy i kierunki rozwoju.

Laboratorium

Opracowanie koncepcji bezpiecznego, sieciowego systemu przechowywania danych dla wybranego środowiska (firmy lub instytucji). Analiza wybranego środowiska, założeń i wymagań dla projektowanego systemu ze szczególnym naciskiem na aspekty bezpieczeństwa tj. poufność, integralność oraz dostępność danych. Wybór odpowiedniej architektury systemu, protokołów, urządzeń sieciowych, oprogramowania, systemów wykonania kopii zapasowych, archiwizacji oraz trwałego usuwania danych w projektowanym systemie. Opracowanie dokumentacji projektowanego systemu. Oszacowanie bezpieczeństwa systemu. Uwzględnienie w projekcie najnowszych technologii w zakresie ochrony danych i obowiązujących przepisów prawa dotyczących przetwarzania danych.

Metody dydaktyczne

Wykład z prezentacją multimedialną. Omawianie regulacji prawnych, interpretacja przepisów, przedstawianie przykładów naruszeń przepisów. Prowadzenie dyskusji w trakcie wykładu. Dodatkowe materiały udostępnione w systemie elearningu.

Laboratorium prowadzone w formie konsultacji i weryfikacji kolejnych zadań. Zadania wykonywane w zespołach 2-osobowych przy użyciu sprzętu komputerowego, narzędzi informatycznych oraz Internetu.

Literatura

Podstawowa

T. Bilski, Pamięć: nośniki i systemy przechowywania danych, WNT, Warszawa, 2008 (sygnatura w Bibliotece PP: W 119644).

J. W. Toigo, Zarządzanie przechowywaniem danych w sieci, Helion, Gliwice, 2004 (sygnatura w Bibliotece PP: W 109697).

S. Nelson, Profesjonalne tworzenie kopii zapasowych i odzyskiwanie danych, Helion, 2012 (sygnatura w Bibliotece PP: W 135831).

Uzupełniająca

Z. Fryźlewicz, D. Nikończuk, Windows Azure. Wprowadzenie do programowania w chmurze, Helion, 2012.

P. Metzger, A. Jełowicki, Anatomia PC, Wyd. Helion, Gliwice, 1998 (lub wydanie nowsze)

F. Schmidt, SCSI i IDE. Protokoły, zastosowania i programowanie, Mikom, 1999.

T. Bilski, Quantitative Risk Analysis for Data Storage Systems, 20th International Conference, CN 2013 Proceedings, [A. Kwiecień, P. Gaj, P. Stera, Editors] Communications in Computer Science and Information Science 370, Springer Verlag, Heidelberg, 2013, s. 124-135.

T. Bilski, Network Storage Systems with IPSec Implementations, Information Systems Architecture and Technology, Networks Design and Analysis, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2012, 127-136

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2
Praca własna studenta (studia literaturowe, elearning, przygotowanie do kolokwium, przygotowanie do laboratorium, przygotowanie dokumentacji realizowanych zadań)[1]	55	2

[1] niepotrzebne skreślić lub dopisać inne czynności