CENTRUM DOSKONALENIA NAUCZYCIELI W PILE

Program szkolenia

Jak zorganizować szkolna infrastrukturę informatyczną (sieć informatyczną)

Opracowali:

Roman Frąckowiak
Piotr Halama
Sławomir Kozłowski

Piła, 2014

PROGRAM WYKŁADU

Polityka bezpieczeństwa infrastruktury IT w szkole/placówce

Liczba godzin: 2

Cel ogólny:

Kształtowanie kompetencji dyrektorów i nauczycieli W zakresie realizacji polityki bezpieczeństwa infrastruktury IT w szkole/placówce.

Cele szczegółowe:

1. Poszerzenie wiedzy na temat polityki bezpieczeństwa sieci informatycznej.
2. Uświadomienie sobie celów i zasad funkcjonowania polityki bezpieczeństwa infrastruktury IT w szkole/placówce.
3. Poszerzanie wiedzy na temat zasad bezpieczeństwa, zakresu odpowiedzialności użytkowników i zabezpieczeń danych w sieci informatycznej.

Treści:

1. Polityka bezpieczeństwa sieci informatycznej.
    - Obszary bezpieczeństwa informacji w szkole/placówce.
    - Składowe systemu informacyjnego.
    - Cele i zasady funkcjonowania polityki bezpieczeństwa.
2. Bezpieczeństwo pracy w sieci informatycznej.
    - Zasady bezpieczeństwa podczas pracy w sieci informatycznej.
    - Zakresy odpowiedzialności użytkowników sieci.
    - Zabezpieczenie danych w sieci informatycznej.

Metody pracy:

- wykład połączony z prezentacją,
- dyskusja.

Projektowanie systemu i procedur bezpieczeństwa szkolnej sieci informatycznej

ROGRAM SZKOLENIA DLA DYREKTORÓW SZKÓŁ/PLACÓWEK

Liczba godzin: 6 (2 części po 3 godziny)

Cel ogólny:

Kształtowanie i rozwijanie kompetencji dyrektorów szkół/placówek w zakresie projektowania bezpieczeństwa szkolnej infrastruktury informatycznej.

Cele szczegółowe:

1. Poszerzenie wiedzy na temat strategii bezpieczeństwa informacji i realizacji polityki bezpieczeństwa szkolnej sieci informatycznej.
2. Uświadomienie sobie zagrożeń w zakresie bezpieczeństwa infrastruktury IT w szkole/placówce.
3. Rozwijanie umiejętności analizy ryzyka w zakresie bezpieczeństwa szkolnej sieci informatycznej.
4. Poszerzenie wiedzy na temat aspektów prawnych prowadzenia polityki bezpieczeństwa.
5. Poszerzenie umiejętności w projektowaniu elementów systemu i procedur bezpieczeństwa szkolnej sieci informatycznej.

Treści:

Część 1.

1. Strategia bezpieczeństwa w szkole/placówce.
    - identyfikacja (diagnoza) potrzeb zapewnienia bezpieczeństwa infrastruktury informatycznej,
    - określenie celu głównego i celów cząstkowych bezpieczeństwa infrastruktury informatycznej,
    - identyfikacja perspektywy realizacji strategii bezpieczeństwa .
2. Sposoby realizacji strategii bezpieczeństwa w szkole/placówce.
    - określenie odpowiedzialności osób i narzędzi realizacji strategii,
    - wyznaczenie etapów realizacji strategii,
    - określenie zagrożeń i czynników sukcesu realizacji strategii.

3. Realizacja polityki bezpieczeństwa infrastruktury IT w szkole/placówce.
    - analiza przypadku realizacji polityki bezpieczeństwa infrastruktury IT w szkole/placówce.
4. Zasady bezpieczeństwa infrastruktury IT w szkole/placówce:
    - Odpowiedzialności i kontroli dostępu do informacji.
    - Bezpieczeństwa kanałów wymiany informacji.
    - Ciągłości działań systemów informatycznych.
    - Ochrony przed czynnikami szkodliwymi.
    - Bezpieczeństwa formalno – prawnego.
    - Zarządzania ryzykiem związanym z bezpieczeństwem systemu informatycznego.

Część 2.

1. Analiza ryzyka w zakresie bezpieczeństwa infrastruktury IT.
    - Identyfikacja zagrożeń.
    - Określanie wielkości ryzyka.
    - Identyfikacja obszarów wymagających szczególnych zabezpieczeń.
2. Aspekt prawny polityki bezpieczeństwa.
    - analiza uwarunkowań prawnych realizacji polityki bezpieczeństwa infrastruktury informatycznej.
3. Sposoby zabezpieczeń szkolnej infrastruktury:
    - oznaczenie danych, określenie zakresu dostępu do danych i odpowiedzialności pracowników za dane – zasada minimalnych uprawnień i ograniczonego dostępu,
    - wielopoziomowość i równoległość zabezpieczeń infrastruktury – określenie poziomów zabezpieczeń infrastruktury IT,
    - zabezpieczenie stacji roboczych i sieci bezprzewodowej (wdrożony system aktualizacji systemu operacyjnego oraz jego składników, zabezpieczenie hasłem, zainstalowane systemy typu: firewall oraz antywirus, konfiguracja kont dostępu z określonymi zakresami uprawnień; zasady korzystania z sieci bezprzewodowej – zakresy uprawnień),
    - polityka w zakresie wykorzystania haseł dostępu do kont (zmienność haseł w czasie, bezpieczeństwo stosowania haseł, tworzenie bezpiecznych haseł dostępu),

- kopie bezpieczeństwa danych (archiwizacja danych, bezpieczne nośniki danych, okresowe testy kopii pod względem możliwości odtworzenia danych),
- monitoring bezpieczeństwa (analiza oprogramowania i zasobów pod względem legalności, analiza ruchu sieciowego komunikacji szkodliwej dla bezpieczeństwa, analiza odwiedzanych stron WWW).

4. Projektowanie elementów systemu i procedur bezpieczeństwa szkolnej sieci informatycznej:
    - sporządzanie procedur bezpieczeństwa w szkolnej infrastruktury informatycznej uwzględniającej zasady: poufności informacji, integralności informacji, dostępności informacji i rozliczalności operacji wykonywanych na informacji,
    - sporządzanie dokumentacji związanej z naruszeniem zasad bezpieczeństwa,
    - weryfikacja przestrzegania procedur bezpieczeństwa sieci informatycznej.

Metody pracy:

- wprowadzenie - mini wykład połączony z prezentacją,
- studium przypadku,
- praca w grupach,
- dyskusja.

Przydatność szkolenia w pracy dyrektora:

Wypracowane podczas warsztatów system i procedury w zakresie strategii i polityki bezpieczeństwa szkolnej infrastruktury IT umożliwią dyrektorom praktyczne ich zastosowanie w procesie zarządzania szkołą/placówką.

Zastosowanie aktywizujących metod pracy pozwoli dyrektorom na wymianę doświadczeń i wspólne przepracowanie kwestii problemowych.

Jak zorganizować szkolną strukturę informatyczną

PROGRAM SZKOLENIA DLA NAUCZYCIELI INFORMATYKI

Liczba godzin: 6

Cele ogólne:

1. Nabycie umiejętności administrowania, utrzymania, zarządzania szkolną infrastrukturą IT na poziomie podstawowym.
2. Nabycie umiejętności korzystania ze sprzętu i oprogramowania dla użytkowników końcowych.
3. Poznanie zasad bezpiecznego korzystania z zasobów Internetu – Security Awareness.

Cele szczegółowe:

1. Zapoznanie ze strukturą szkolnej infrastruktury IT.
2. Zapoznanie z systemami i standardami cyfrowej transmisji bezprzewodowej.
3. Zapoznanie z administracją sieciami opartymi na systemie Windows i Linux.
4. Konfiguracja sieci bezprzewodowych i przewodowych.
5. Projektowanie dostępu do zasobów oraz przyłączanie dodatkowych zasobów.
6. Wykonywanie czynności związanych z przygotowaniem środowiska bezpiecznej pracy użytkowników sieci komputerowej (np. ochrony antywirusowej, tworzenia awaryjnych dysków naprawczych).
7. Konfigurowanie i administrowanie serwerami: WWW, FTP, pocztowym, baz danych (w tym konfigurowania serwerów wirtualnych oraz rozszerzanie serwerów o funkcjonalność obsługi dodatkowych języków (np. PHP).
8. Generowanie zaufanych certyfikatów SSL.
9. Nabycie umiejętności udostępniania zasobów: na serwerze lokalnym w chmurze, e-zasobów oraz na platformie Moodle.
10. Nabycie umiejętności pracy z interaktywnymi zasobami dydaktycznymi w oparciu o wykorzystanie tablicy interaktywnej.
11. Wdrażanie elementów polityki bezpieczeństwa.

Treści kształcenia:

Moduł I – 3h

Sieci oparte na systemie Windows i Linux

- Architektura systemu Windows i Linux**.**
- Instalacja systemu w warunkach nietypowych.
- Postępowanie w typowych sytuacjach awaryjnych.
- Zastosowanie technologii zasad grup w zarządzaniu komputerami oraz środowiskiem użytkownika.
- Kopie bezpieczeństwa.
- Obsługa zdalna serwera.
- Przykłady rozwiązań ułatwiających administrację szkolną siecią komputerową (DHCP, DNS).

Moduł II – 2 h

E-szkoła, e-zasoby

- Wykorzystanie nowoczesnych technologii do budowania zasobów edukacyjnych szkoły (serwer szkolny z zasobami edukacyjnymi, platforma edukacyjna np. moodle, e-dziennik).
- Wykorzystanie TIK w pracy dydaktycznej (tablet, smartfon, tablica multimedialna).

Moduł III – 1h

Bezpieczeństwo w sieci

- Certyfikaty SSL.
- Zabezpieczanie danych, haseł i loginów.
- Procedury bezpiecznego przepływu informacji.
- Strategia bezpieczeństwa informatycznego w szkole.

Sposoby realizacji:

Formy:

- indywidualna

Metody:

- wykład
- ćwiczenia przy komputerze
- dyskusja

Przydatność zakładanych efektów szkolenia w pracy nauczyciela:

- Zwiększenie umiejętności zarządzania sieciami opartymi na strukturze Windows i Linux.
- Wykorzystanie nowoczesnych technologii związanych z realizacją zadań szkoły dotyczących umożliwiania zdobywania wiedzy i umiejętności.
- Wdrożenie bezpiecznej strategii bezpieczeństwa infrastruktury w szkole oraz przechowywania danych.
- Przygotowanie własnej bazy dydaktycznej szkoły oraz udostępnienie zasobów uczniom poprzez serwer danych i platformę edukacyjną (moodle, Live@edu).

Zalecana literatura przedmiotu:

1. Sieci VPN. Zdalna praca i bezpieczeństwo danych, Marek Serafin, Helion 2012,
2. Sieci komputerowe. Biblia. Barrie Sosinsky, Helion, 2011
3. Internet. Ilustrowany przewodnik, Radosław Sokół, Helion 2007,
4. William H. Rice IV, *Tworzenie serwisów e-learningowych z Moodle 1.9*, Helion 2010
5. Tablice interaktywne w procesie nauczania [13.03.2008] http://www.edunews.pl/
6. Zamiast zwykłej szkolnej tablicy [25.09.2008] http://www.edunews.pl/
7. Pożegnanie ze stara edukacja? [25.04.2009] http://www.edunews.pl/
8. http://www.e-edukacja.net/
9. http://www.czn.uj.edu.pl/moodle/
10. http://www.edunews.pl/
11. http://szupa.w.interia.pl/podstrony/topologie.html
12. http://sieci_komputerowe.w.interia.pl/referaty/referat10.html

ROGRAM SZKOLENIA DLA NAUCZYCIELI PRZEDMIOTÓW NIEINFORMATYCZNYCH

Liczba godzin: 6
Cel ogólny:

Wykorzystanie szkolnej infrastruktury informatycznej przez nauczycieli przedmiotów nieinformatycznych.

Cele szczegółowe:
uczestnik po zajęciach:

1. Umie wykorzystywać sprzęt i oprogramowanie dostępne w szkole.
2. Potrafi instalować dodatkowe – darmowe oprogramowanie na dostępnych systemach operacyjnych windows/linux/android.
3. Zna rodzaje i zasadę działania sieci bezprzewodowych.
4. Potrafi podłączyć sprzęt typu laptop/tablet do sieci bezprzewodowej,
5. Zna typowe problemy związane z funkcjonowaniem (łącznością) sieci bezprzewodowych.
6. Potrafi stworzyć własną (mobilną) sieć bezprzewodową.
7. Stosuje zasady bezpieczeństwa przy korzystaniu z zasobów Internetu oraz sprzętu ogólnodostępnego w szkole.

Treści:

1. Uruchomienie i obsługa sprzętu.
2. Instalacja i uruchamianie programów na różnych systemach operacyjnych.
3. Rodzaje i zasada działania sieci bezprzewodowych.
4. Podłączenie sprzętu do sieci bezprzewodowej - konfiguracja urządzeń klienckich laptop / tablet.
5. Wykorzystanie Internetu na urządzeniach typu laptop / tablet.
6. Mechanizmy zabezpieczeń sieci bezprzewodowych.
7. Mobilne sieci bezprzewodowe.
8. Security Awareness – podstawy bezpieczeństwa.
9. Bezpieczny pendrive – szyfrowanie danych.

Metody i formy pracy:

- praca warsztatowa
- dyskusja

Przydatność zakładanych efektów szkolenia w pracy nauczyciela

Do realizacji szkolenia wykorzystane zostaną informacje, uzyskane od uczestników, dotyczące sprzętu i oprogramowania dostępnego w ich szkołach. Takie podejście pozwoli uczestnikom dokonać refleksji nad własnym warsztatem pracy i umożliwi w pełni wykorzystać poznane umiejętności podczas własnej pracy.

Poruszane treści dotyczą bieżących problemów, z którymi nauczyciele muszą borykać się codziennie w swojej pracy. Zdobyte umiejętności będą mogli wykorzystywać w konkretnych szkolnych sytuacjach. Szkolenie pomoże im także samodzielnie rozwiązywać typowe problemy związane z obsługą sprzętu i oprogramowania dostępnego w szkołach i odpowie na nurtujące ich pytania. Zagadnienia związane z obsługą sieci bezprzewodowych oraz Security Awareness pozwolą nauczycielom na bezpieczną wymianę informacji i danych w szkolnych sieciach.