



Temat: SRU – Jak chronić ważne informacje

Opis istoty zajęć:

Zaawansowane użytkowanie Linuksa, podstawowe informacje o bezpieczeństwie danych i szyfrowaniu.

Autor:

Adam Jurkiewicz **Proponowany czas realizacji:** 90

Cele:

1. ogólne (zadanie/przesłanie nauczyciela dla całych zajęć):

ukształtowanie wiedzy o bezpieczeństwie danych i szyfrowaniu; rozwijanie kreatywności i innowacyjności; poznanie różnych aplikacji i szyfrowania PGP;

2. szczegółowe: uczennica/uczeń

- posiada wiedzę z zakresu obsługi linii poleceń i szyfrowania;
- rozwinię umiejętność poruszania się w środowisku Linuksa;
- posiada wiedzę z zakresu szyfrowania danych i używania podpisu elektronicznego.

Metody działania:

- pogadanka i dyskusja – rozpisanie na kartce szyfru analogicznego, jak ROT-13;
- prezentacja multimedialna – zapoznanie z oprogramowaniem;
- metoda ćwiczebna – tworzenie własnych kluczy PGP, podpisywanie i szyfrowanie wiadomości.

Wskaźniki osiągnięcia celów (efekty): uczennica/uczeń

- wskaże wagę bezpieczeństwa danych oraz zalety podpisu elektronicznego i szyfrowania;
- omówi sposoby zdobywania informacji z manuali systemowych;
- omówi obsługę konsoli;
- wykorzysta podstawowe funkcje obsługi Linuksa, aplikacji gpg, Kggpg;
- utworzy własne klucze pgp, nauczy się obsługi gpg z linii poleceń.

Czynności uczniów	Działania trenera	Materiały i środki
Uczestniczą w pogadance.	Wprowadza do tematu: zachęca uczennice/uczniów do zastanowienia się, czy mają jakieś ważne informacje, które chcieliby szyfrować (np. hasła); wskazuje, do czego możemy wykorzystywać podpis elektroniczny (ważne pisma, ważne dane). Omawia zalety podpisu elektronicznego i szyfrowania - pogadanka.	Pojęcia: szyfrowanie, bezpieczeństwo danych, podpis elektroniczny.
Wspólnie z nauczycielem rozpisują szyfr analogiczny do ROT-13 i w ten sposób zapoznają się ze schematem listy danych i wskaźników (do elementów listy).	Omawia metody ROT-13 dla prostego szyfrowania; rozpisuje na kartce szyfru analogiczny, jak ROT-13.	ROT-13 http://pl.wikipedia.org/wiki/ROT13



Współuczestniczą w pokazie, zadają pytania, wyjaśniają wątpliwości.	Prezentuje funkcje oprogramowania gpg (man systemowy) – prezentacja multimedialna.	Opisy technologii PGP: http://pl.wikipedia.org/wiki/GPG oraz http://pl.wikipedia.org/wiki/Pretty_Good_Privacy oraz podręcznik systemowy gpg (man gpg).
Tworzą własne klucze gpg, eksportują je na serwer kluczy w internecie, pobierają klucze kolegów/koleżanek, kopiują sobie nawzajem pliki.	Formułuje zadania:Utwórz własną parę kluczy PGP i wyeksportuj je na serwer kluczy;Odnajdź na serwerze kluczy i zaimportuj klucz (adam.jurkiewicz@fwioo.pl) oraz klucze kolegów i koleżanek z zajęć;Stwórz tekst,zaszyfruj go i przekaż do odszyfrowania.Wspiera uczniów podczas tworzenia własnych kluczy PGP, podpisywania i szyfrowania wiadomości.	

