



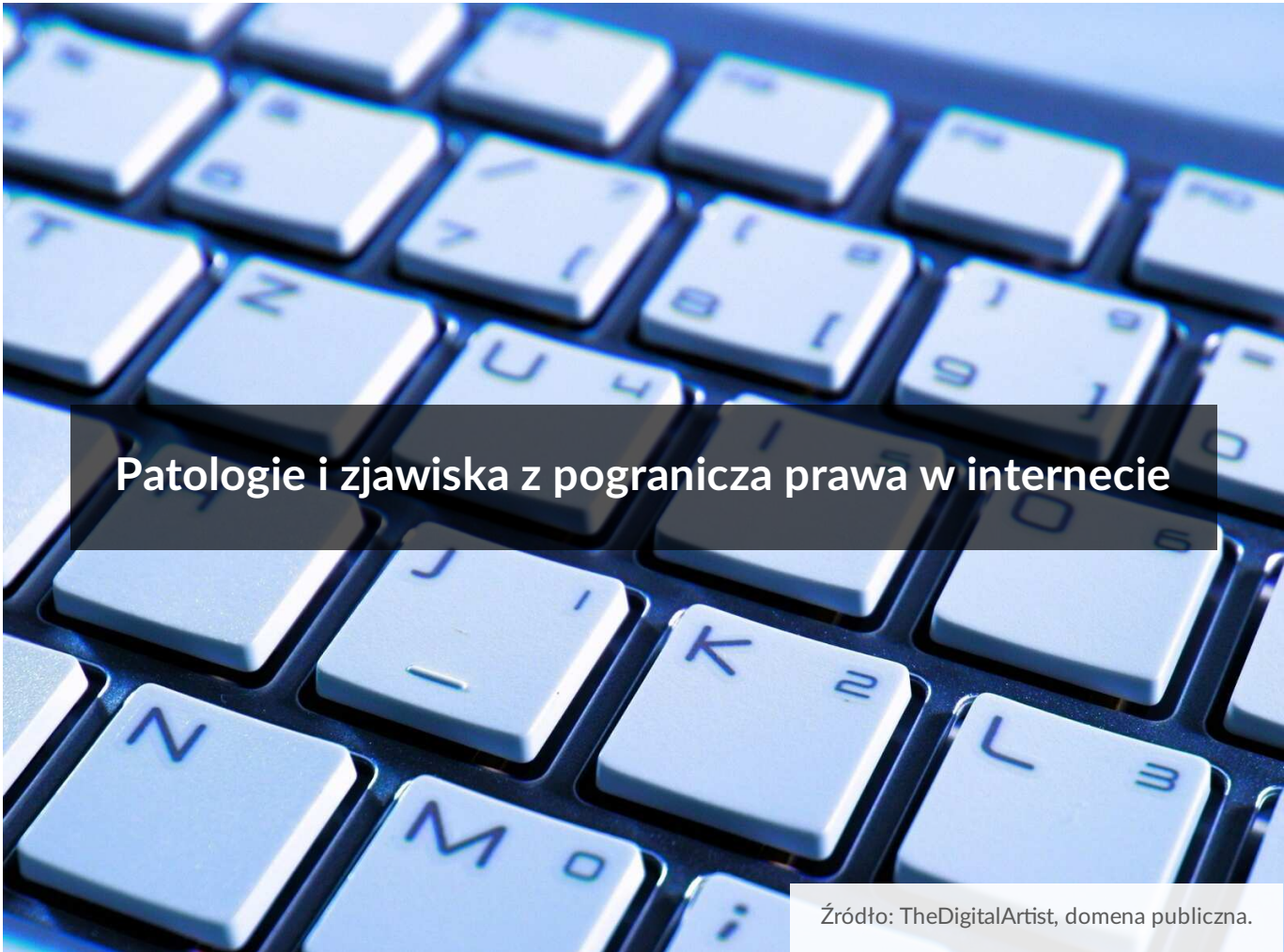
Patologie i zjawiska z pogranicza prawa w internecie

- [Wprowadzenie](#)
- [Przeczytaj](#)
- [Gra edukacyjna](#)
- [Sprawdź się](#)
- [Dla nauczyciela](#)

Bibliografia:

- Źródło: *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].
- Źródło: *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii*, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].

- Źródło: *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 27 października 1932 r. Prawo o broni, amunicji i materiałach wybuchowych*, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].
- Źródło: Maciej Siwicki, *Cyberprzestępczość*, 2013.



Patologie i zjawiska z pogranicza prawa w internecie

Źródło: TheDigitalArtist, domena publiczna.

Nowe technologie towarzyszą nam dziś właściwie na każdym kroku. Nie wyobrażamy sobie życia bez internetu, z którego korzystamy, np. wykonując operacje bankowe czy robiąc zakupy. Śmiało można rzec, że internet stanowi nieodzowną część naszego świata. Rozwój technologii stale otwiera nowe możliwości.

Jednak oprócz niewątpliwych korzyści, jakie płyną z informatyzacji, internet niesie za sobą również zagrożenia. Nikogo nie dziwią już przestępstwa internetowe. Czy sieć jest zatem ziemią niczyją, na której panuje bezprawie?

Więcej informacji o ciemnych obliczach internetu znajdziesz w e-materiałach:

- [Przestępczość komputerowa](#),
- [Treści szkodliwe w internecie](#),
- [Sieć ukryta](#).

Twoje cele

- Wskażesz patologie i zjawiska z pogranicza prawa w internecie.
- Scharakteryzujesz anonimowość w sieci.
- Przeanalizujesz cechy przestępstw handlu ludźmi, handlu narkotykami czy terroryzmu.

Przeczytaj

Anonimowość w sieci

Internet przez sporą grupę użytkowników uważany jest za bezpieczne miejsce, w którym można czuć się w pełni anonimowo. I to właśnie owa pozorna anonimowość przyczynia się do rozkwitu przestępczości w sieci. Wciąż pojawiają się nowe formy [przestępstw](#) komputerowych, ponieważ internet stwarza idealne warunki do ich funkcjonowania i rozwoju.

Sposoby na pozostanie anonimowym w sieci:

- VPN (z ang. *Virtual Private Network*) – polega na szyfrowaniu połączenia pomiędzy dwiema sieciami. Sieć VPN umożliwia anonimowe przeglądanie stron internetowych;
- serwery proxy – serwery pośredniczące, które uczestniczą w wymianie informacji na linii komputer – serwer docelowy. W tym przypadku anonimowość nie jest pełna, bowiem serwer proxy może zapisywać informacje o źródle połączenia, dzięki czemu możliwa jest identyfikacja użytkownika;
- przeglądarka Tor – wirtualna sieć komputerowa, w której przesyłane dane są wielowarstwowo szyfrowane, a węzły wybierane losowo, dlatego też dla strony, z której korzystasz, możesz wydawać się użytkownikiem z drugiego końca świata.

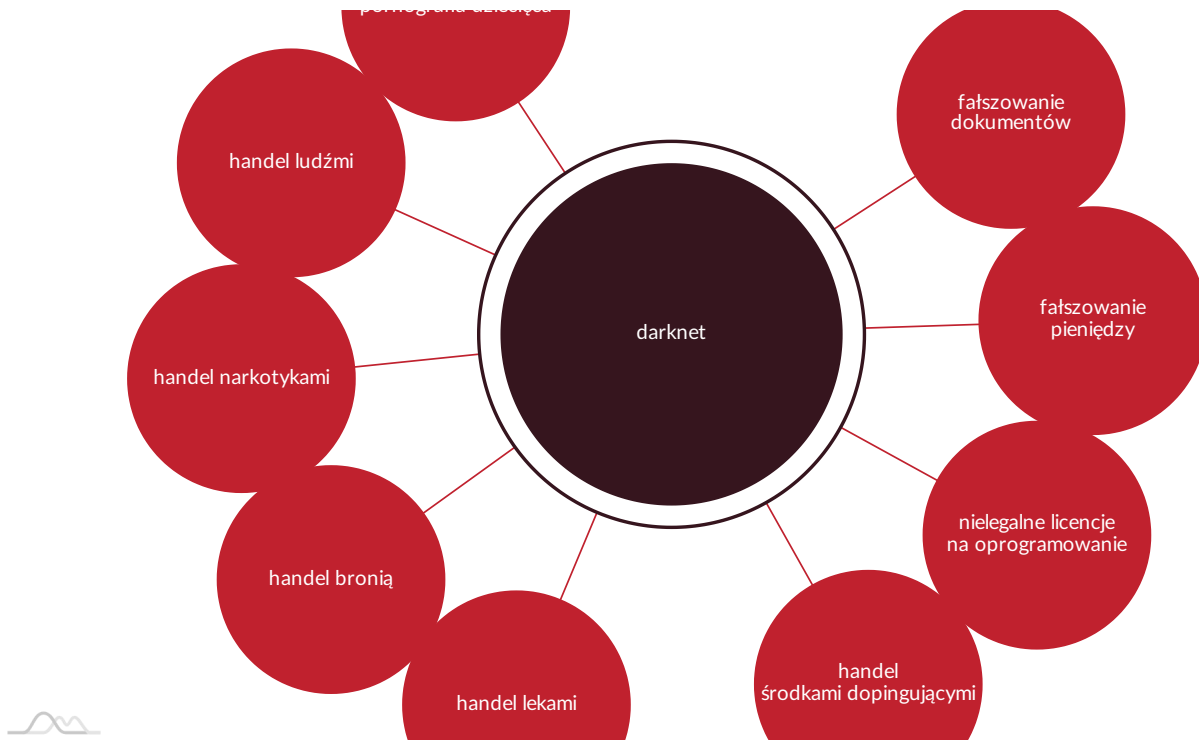
Polecenie 1

Poszukaj informacji o tym, w jaki sposób w sieci zostawiamy po sobie ślad. Do czego mogą być używane dane zbierane na jego podstawie?

Darknet – ciemna strona internetu

Darknet to ogólne określenie wszystkich anonimowych stron internetowych, sklepów czy innych serwisów, które są dostępne w sieci. Co je odróżnia stron internetowych dostępnych dla wszystkich użytkowników? To, że nie można ich znaleźć przez

powszechnie używane wyszukiwarki oraz że nie są dostępne przez adres WWW. Niezbędna jest więc specjalna przeglądarka, np. Tor. Ukryta sieć to idealne miejsce dla cyberprzestępców. Można tutaj kupić praktycznie wszystkie towary i usługi – zarówno legalne, jak i nielegalne.



Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

Nie można kategorycznie stwierdzić, że darknet to miejsce wyłącznie dla przestępców, bo wykorzystywane jest również do słuszych celów, np. do komunikacji w krajach, które nakładają na swoich obywateli cenzurę. Przykładem takiego państwa mogą być Chiny.

Handel bronią

” Rozporządzenie Prezydenta Rzeczypospolitej z dnia 27 października 1932 r. Prawo o broni, amunicji i

materiałach wybuchowych

Art. 4. (1) Bronią i amunicją wolno zawodowo handlować tylko na zasadzie pozwolenia władzy.

(2) Przedsiębiorstwa wytwórcze mogą sprzedawać wytwarzaną przez siebie broń lub amunicję bez pozwolenia:

- osobom posiadającym pozwolenie na handel bronią i amunicją (ust. 1) oraz
- na zamówienie - osobom uprawnionym do nabywania broni lub amunicji zgodnie z przepisami niniejszego prawa.

Źródło: Rozporządzenie Prezydenta Rzeczypospolitej z dnia 27 października 1932 r. Prawo o broni, amunicji i materiałach wybuchowych, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].

Tyle z teorii – teraz rzeczywistość. Obecnie każdy może kupić nielegalną broń w darknecie. Co więcej, ani sprzedawca, ani nabywca nie ujawniają swojej tożsamości. Kiedyś handlem bronią zajmowały się [zorganizowane grupy przestępcze](#), dziś można dokonać zakupu nawet u pojedynczego kryminalisty, co obrazuje skalę przestępczego działania. Aby dostać się na internetowy bazar z bronią, trzeba skorzystać ze sposobów zapewniających anonimowe korzystanie z sieci. Jedynym wymaganiem, jakie muszą spełnić obie strony transakcji, jest zbudowanie wzajemnego zaufania. Przeglądarka Tor wychodzi tu naprzeciw oczekiwaniom użytkowników i umożliwia przeglądanie dotychczasowych transakcji oraz ocen partnera handlowego, co pozwala zweryfikować jego wiarygodność.

Handel narkotykami

W polskim porządku prawnym handel narkotykami jest zabroniony pod groźbą kary.

” Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii

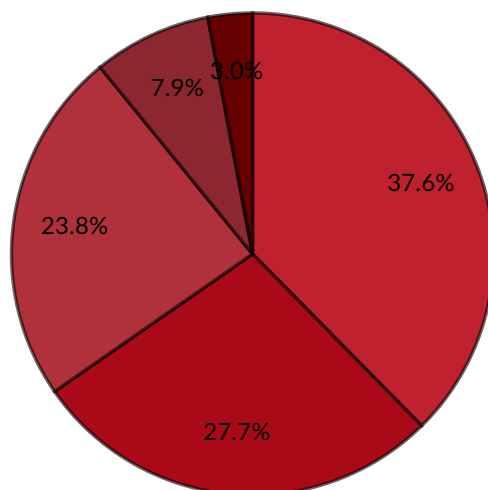
Art. 58. [Udzielanie innej osobie środka odurzającego. Nakłanianie do użycia środka]

1. Kto wbrew przepisom ustawy udziela innej osobie środka odurzającego, substancji psychotropowej lub nowej substancji psychoaktywnej, ułatwia albo umożliwia ich użycie albo nakłania do użycia takiego środka lub substancji, podlega karze pozbawienia wolności do lat 3.

Źródło: Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].

Handel narkotykami to biznes odpowiadający za blisko jedną piątą światowych wpływów z nielegalnej działalności. Liczba stron internetowych, za pośrednictwem których można kupić narkotyki, jest zatrważająca. Sprzedawcy proponują różnego rodzaju promocje, np. rabaty ilościowe, wysyłkę z wyborem opcji dostawy, a w przypadku zaginięcia paczki – ponowną wysyłkę czy też korzystne zasady reklamacji.

Udział w rynku narkotykowym w UE



konopie indyjskie 37.6% heroina 27.7% kokaina 23.8% amfetamina 7.9%
ecstasy 3.0%

Uwaga: W związku z zaokrąglaniem liczb ich suma nie wynosi 100%.

Oprac. na podst.: Europol, *Raport o rynku narkotykowym w UE. Przegląd strategiczny*, emcdda.europa.eu [online, dostęp: 8.12.2020].

Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

Terroryzm

” Ustawa z dnia 6 czerwca 1997 r. Kodeks karny

§ 20. Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1. poważnego zastraszenia wielu osób;
2. zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności;

3. wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej;

– a także groźba popełnienia takiego czynu.

Źródło: Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].

Obecnie podstawowym narzędziem w rękach terrorystów jest internet. Wykorzystuje się go do komunikacji, przeprowadzania szkoleń, doradztwa czy nawet werbunku. Aby zapobiec rozpowszechnianiu się terroryzmu w sieci, w Niemczech utworzono Wspólne Centrum Internetowe, które ma za zadanie monitorować treści pojawiające się online. Centrum nie prowadzi jednak dochodzeń – jego działalność opiera się na analizie danych, które potem są przekazywane policji.

W 2007 roku przy Europolu utworzono portal informacyjny, za pośrednictwem którego wszystkie państwa Unii Europejskiej mogą dokonywać wymiany informacji na temat przestępstw terrorystycznych.

Handel ludźmi

” Ustawa z dnia 6 czerwca 1997 r. Kodeks karny

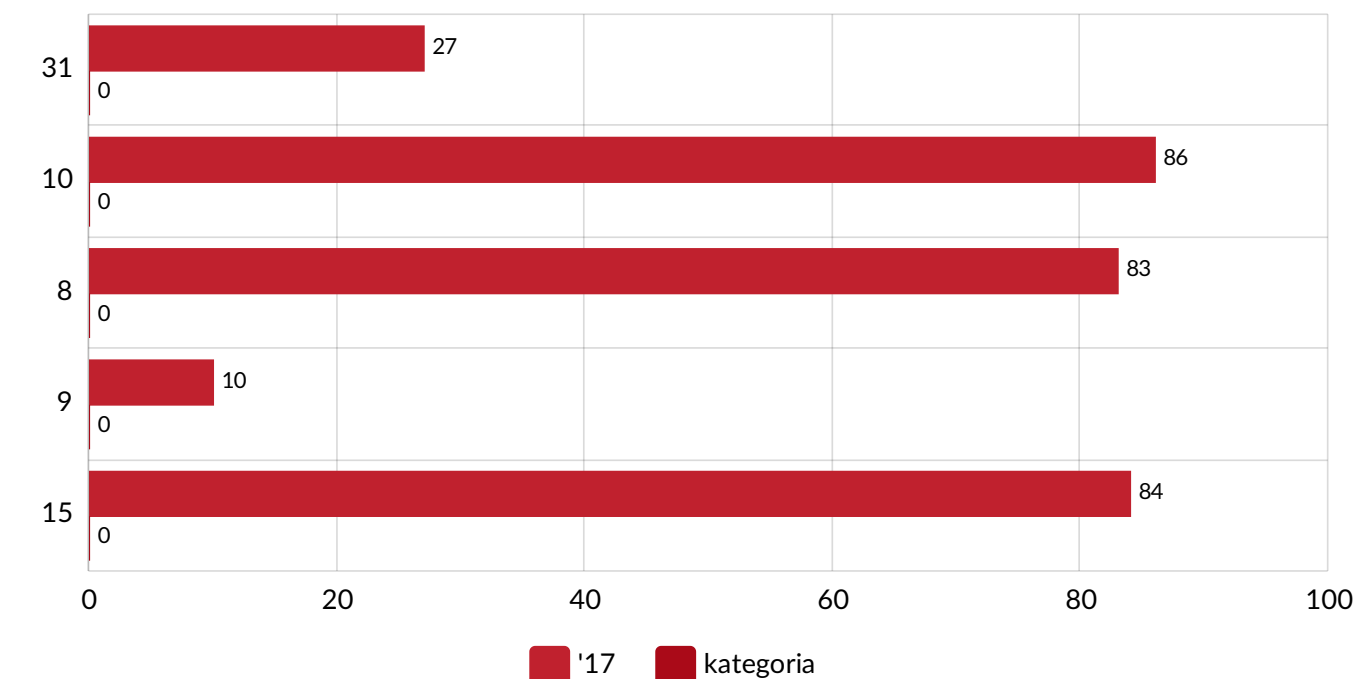
Handlem ludźmi jest werbowanie, transport, dostarczanie, przekazywanie, przechowywanie lub przyjmowanie osoby z zastosowaniem:

1. przemocy lub groźby bezprawnej;
2. uprowadzenia;
3. podstępu;
4. wprowadzenia w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania;

5. nadużycia stosunku zależności, wykorzystania krytycznego położenia lub stanu bezradności;
 6. udzielenia albo przyjęcia korzyści majątkowej lub osobistej albo jej obietnicy osobie sprawującej opiekę lub nadzór nad inną osobą
- w celu jej wykorzystania, nawet za jej zgodą, w szczególności w prostytucji, pornografii lub innych formach seksualnego wykorzystania, w pracy lub usługach o charakterze przymusowym, w żebractwie, w niewolnictwie lub innych formach wykorzystania poniżających godność człowieka albo w celu pozyskania komórek, tkanek lub narządów wbrew przepisom ustawy.

Źródło: Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020].

Handel ludźmi – Przepęstwo z art. 189a § 1-2 k.k. – w latach 2016/17



Oprac. na podst.: *Handel ludźmi w Polsce Raport za 2017 r.*, handelludzmi.eu [online, dostęp: 8.12.2020].

Darknet używany jest przez osoby zajmujące się handlem ludźmi.

Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

Polecenie 2

Poszukaj aktualnych danych odnoszących się do handlu ludźmi. Jaką rolę odgrywa w nim internet nakładkowy?

Słownik

koncesja

akt administracyjny, który upoważnia do prowadzenia określonej działalności gospodarczej

przestępstwo

czyn zawiniony oraz bezprawny, tj. zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia

zorganizowana grupa przestępcza

współpraca przynajmniej trzech osób, których celem jest popełnienie określonych przestępstw, przy czym członkowie nie mają określonych stałych ról i pozycji w hierarchii wewnętrznej grupy

Gra edukacyjna



Test

Sprawdź swoją wiedzę, biorąc udział w grze

Poziom trudności:

łatwy

Limit czasu:

7 min

Twój ostatni wynik:

-

Uruchom

Sprawdź się

Pokaż ćwiczenia:   

Ćwiczenie 1



Wskaż, które stwierdzenia są prawdziwe, a które fałszywe.

Stwierdzenie	Prawda	Fałsz
Każda osoba w dowolnej chwili może rozpocząć wykonywanie działalności gospodarczej w zakresie wytwarzania i obrotu bronią.	☐	☐
Zgoda osoby pokrzywdzonej wyłącza bezprawność przestępstwa handlu ludźmi.	☐	☐
Udostępnianie odpłatne, jak i nieodpłatne narkotyków jest karalne.	☐	☐

Ćwiczenie 2



Wskaż sposoby na pozostanie anonimowym w sieci.

☐ VPN

☐ tryb incognito

☐ nieużywanie własnych zdjęć

☐ przeglądarka Tor

☐ systemy proxy

☐ używanie pseudonimu zamiast nazwiska

Ćwiczenie 3



Połącz każde pojęcie z właściwą definicją.

koncesja

czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia o stopniu szkodliwości większym niż znikomy

zorganizowana grupa przestępcza

akt administracyjny, który upoważnia do prowadzenia określonej działalności gospodarczej

przestępstwo

współpraca przynajmniej trzech osób, których celem jest popełnienie określonych przestępstw, przy czym członkowie nie mają określonych stałych ról i pozycji w hierarchii wewnętrznej grupy

Ćwiczenie 4



Uzupełnij zdania właściwymi elementami.

Przestępstwem o charakterze terrorystycznym jest czyn zabroniony popełniony w celu poważnego zastraszenia osób.

to ogólne określenie wszystkich anonimowych stron internetowych, które dostępne są w sieci.

Serwery pośredniczące, które uczestniczą w wymianie informacji na linii komputer - serwer docelowy, to inaczej serwery .

torrent

Tor

Darknet

wielu

kilku

proxy

Ćwiczenie 5



Wskaż dwa przykłady przestępstw internetowych.

Ćwiczenie 6



Wskaż fałszywą informację.

☐

Dla zaistnienia przestępstwa handlu ludźmi wystarczające jest dokonanie jednej transakcji.

☐

VPN polega na szyfrowaniu połączenie pomiędzy dwiema sieciami.

☐

Serwery proxy zapewniają całkowitą anonimowość.

☐

Handel ludźmi to np. werbowanie osób za pomocą podstępu w celu ich wykorzystania.



Zapoznaj się z tekstem i wykonaj polecenie.

” Maciej Siwicki

Cyberprzestępczość

Wśród powodów wzrostu zagrożenia przestępczością *stricte* komputerową w literaturze przedmiotu najczęściej wymienia się brak stosownej wiedzy na temat nadużyć komputerowych, jak i odpowiedniego oprogramowania, które wykryłoby np. złośliwe oprogramowanie, które często działa w ukryciu, wykorzystuje luki w oprogramowaniu lub aktywuje się dopiero po pewnym czasie (np. bomby logiczne, wirusy, trojany). Wskazuje się również, że cechą charakterystyczną przestępczości *stricte* komputerowej jest niewielka gotowość ofiar przestępstw do angażowania policji w ich ściganie, pomimo relatywnie wysokich szkód, jakie czyny te w ocenie pokrzywdzonych powodują.

Przestępczość komputerową charakteryzują ponadto: duża „ciemna liczba”, niskie prawdopodobieństwo wykrycia sprawcy oraz lekceważenie przez pokrzywdzonych środków bezpieczeństwa. Transfer danych z wykorzystaniem sieci teleinformatycznych zazwyczaj przebiega przez kilka państw. Protokoły wykorzystywane do transferu bazują bowiem na wyszukiwaniu optymalnej trasy omijają np. bezpośrednie połączenia, które mogą być w momencie transferu zablokowane lub przeciążone. Ponadto wiele usług świadczonych drogą elektroniczną może być zlokalizowane (m.in. ze względów ekonomicznych, czy praktycznych) w kilku państwach np. usługodawcy świadczący usługę hostingu mogą ją świadczyć w jedynym państwie korzystając ze sprzętu zlokalizowanego w innym.

Źródło: Maciej Siwicki, *Cyberprzestępczość*, 2013.

Wskaż przykładowe czynniki utrudniające ściganie cyberprzestępców.

Ćwiczenie 8



Wskaż czynności sprawcze przestępstwa handlu ludźmi.

Dla nauczyciela

Autor: Anita Rozik

Przedmiot: Informatyka

Temat: Patologie i zjawiska z pogranicza prawa w internecie

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;

- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Wskażesz patologie i zjawiska z pogranicza prawa w internecie.
- Scharakteryzujesz anonimowość w sieci.
- Przeanalizujesz cechy przestępstw handlu ludźmi, handlu narkotykami czy terroryzmu.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimediu i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;

- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Patologie i zjawiska z pogranicza prawa w internecie”. Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj”.

Faza wstępna:

1. Nauczyciel wyświetla i odczytuje temat lekcji oraz cele zajęć. Prosi uczniów o sformułowanie kryteriów sukcesu.
2. **Rozpoznanie wiedzy uczniów.** Uczniowie tworzą pytania dotyczące tematu zajęć, na które odpowiedzą w trakcie lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu e-materiału. Indywidualnie zapoznają się z treścią w sekcji „Przeczytaj”.
2. Nauczyciel inicjuje dyskusję na temat tego, w jaki sposób działa (i czy w ogóle) anonimowość w sieci. Uczniowie zapoznają się z poleceniami zamieszczonymi w sekcji „Przeczytaj” i odpowiadają na zawarte w nich pytania.
3. Uczniowie rozwiązują ćwiczenia wskazane przez nauczyciela.
4. Uczniowie w grupach przygotowują krótkie prezentacje o tym, w jaki sposób wykorzystywane są dane zbierane na temat użytkowników w sieci.
5. Grupy prezentują przygotowane przez siebie przykłady.
6. Uczniowie w ramach utrwalenia wiadomości rozwiązują test (sekcja „Gra edukacyjna”).

Faza podsumowująca:

1. Uczniowie odpowiadają na pytanie: „Czy w sieci można być anonimowym?”.
Uzasadniają swoją odpowiedź.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 7 i 8 z sekcji „Sprawdź się”.

Wskazówki metodyczne:

- Lekcja wraz z materiałami dot. prawa karnego (WoS) może stanowić ścieżkę międzyprzedmiotową. E-materiały można wykorzystać do przeprowadzenia zajęć warsztatowych (teoretyczne zajęcia dot. prawa karnego połączone z jego aplikacją na gruncie sieci internetowej).