

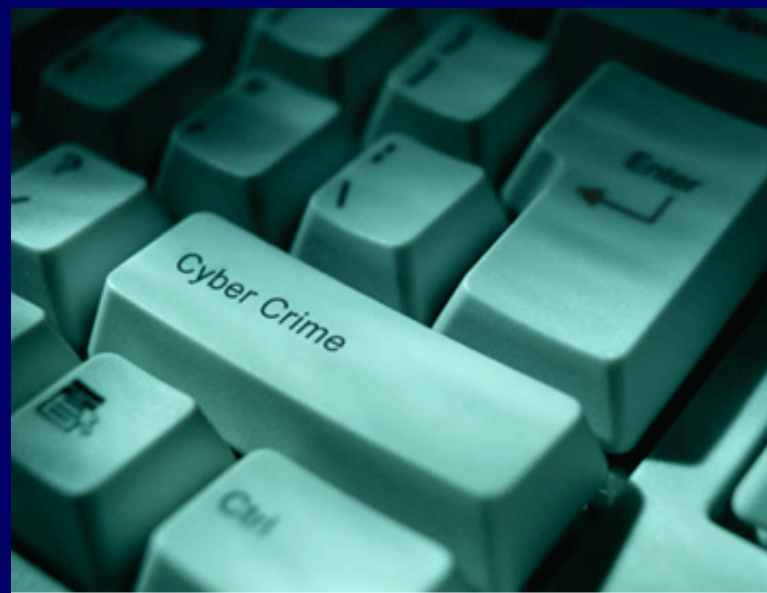


Informatyk w okowach prawa karnego.

Przestępstwa komputerowe od hakingu po posiadanie zabronionego oprogramowania i danych

15 maja 2008 r., Gdańsk

INFOSHARE



dr Wojciech R. Wiewiórowski

Wydział Prawa i Administracji,
Uniwersytet Gdański



Nota:

Niniejsza prezentacja stanowi uzupełnienie wykładu prezentowanego na konferencji „*infoShare 2008*”, która odbyła się na Politechnice Gdańskiej w dniach 14-15 maja 2008 r.

Prezentację można kopiować i wykorzystywać w całości lub w części tylko pod warunkiem podania pełnej informacji o utworze w poniższym brzmieniu:

*W.R. Wiewiórowski, „Informatyk w okowach prawa karnego. Przesłpstwa komputerowe od hakingu po posiadanie zabronionego oprogramowania i danych”, WPIA Uniwersytet Gdański 2008
(wersja z 15 maja 2008 r.)*

Z wersji prezentowanej w sieci usunięto niektóre elementy graficzne możliwe do prezentacji tylko w warunkach dozwolonego użytku publicznego.

© *W.R. Wiewiórowski*

Informatyk w okowach prawa karnego

Pracownia Informatyki Prawniczej
Wydział Prawa i Administracji
Uniwersytetu Gdańskiego



dr Wojciech R. Wiewiórowski



ul. J. Bażyńskiego 6, pok 1032
80-952 Gdańsk
+48-58-523 29 76

wojciech.wiewiorowski@mswia.gov.pl

dr Wojciech R. Wiewiórowski

Wydział Prawa i Administracji,
Uniwersytet Gdański



Informatyk w okowach prawa karnego

0. Przestępstwo ?

1. Posiadanie oprogramowania i danych hakerskich.

Prawnicze rozumienie terminu haking.

- Karalność posiadania w prawie polskim na przykładzie posiadania broni i posiadania „twardej” pornografii.
- Regulacje międzynarodowe (Unia Europejska, Rada Europy).
- Co jest zabronione?
- Czy prawo może być mechanizmem szantażu?
- Omówienie dostępnych w Polsce produktów i usług, które są de facto zakazane przez kodeks karny.
- Niemcy podążają drogą Polski (zmiany w niemieckim prawie karnym z maja 2007 r.)
- Policjant jako haker.

2. Posiadanie narzędzi i ich komponentów oraz oprogramowania służącego do usuwania tzw. skutecznych zabezpieczeń.

- Prawna regulacja Digital Rights Management.
- „Skuteczne zabezpieczenia utworów”.
- Zmiany proponowane przez Ministerstwo kultury i Dziedzictwa Narodowego.
- Czym jest w prawie polskim „program komputerowy”.
- Kryptolog jako przestępca.
- Co to jest zorganizowana grupa przestępcza?
- Przykład praktyczny – „Konferencja kryptologów widziana jako zgromadzenie organizacji o charakterze przestępczym”.



3. Różne formy hakingu.

- Prawnicze rozumienie terminu haking – podsumowanie.
- Interpol o hakingu.
- Rada Europy o hakingu – Konwencja budapeszteńska o cyberprzestępczości.
- Unia Europejska o hakingu – decyzja ramowa o atakach na systemy.
- Haking a ochrona korespondencji.
- Dlaczego w kodeksie karnym potrzebne są zmiany.
- Zaostrzenie ścigania hakingu przy jednoczesnej eliminacji ścigania duchów.

4. Organizacje przestępcze

- Związek przestępczy
- Zorganizowana grupa przestępcza
 - **Dlaczego PTI powinno być traktowane jako związek przestępczy**

0. Czym właściwie jest „przestępstwo”



- Czyn
- Kryminalnie bezprawny
- Społecznie szkodliwy w stopniu więcej niż znikomym
- Zawiniony

0. Czym właściwie jest „przestępstwo”



Formy winy

- umyślność
 - ✓ zamiar bezpośredni (przemysłany i nagły)
 - ✓ zamiar ewentualny
- nieumyślność
 - ✓ nieumyślność świadoma (lekkomyślność)
 - ✓ nieumyślność nieświadoma (niedbalstwo)



1. Podstawy prawne

Konwencja Rady Europy o cyberprzestępczości podpisana w Budapeszcie 23 listopada 2001 r.

- Polska podpisała konwencję i przygotowuje się do jej ratyfikacji
- Kodeks karny został (teoretycznie) dostosowany do konwencji poprzez tzw. „cybernowelizację” z 2004 r.



1. Podstawy prawne

Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady
z dnia 22 maja 2001 r.
w sprawie harmonizacji niektórych aspektów praw autorskich
i pokrewnych w społeczeństwie informacyjnym
(Dz.U.UE L z dnia 22 czerwca 2001 r.)

Wejście w życie: 22 czerwca 2001 r. - dla Unii Europejskiej

Termin implementacji: 22 grudnia 2002 r.

Wejście w życie: 1 maja 2004 r. - dla Polski



1. Wskazania dyrektywy

Istnieje (...) ryzyko rozwoju nielegalnych form działalności zmierzających do umożliwienia lub ułatwienia obchodzenia zabezpieczenia technicznego (...). W celu uniknięcia wyrywkowych podejść prawnych, które mogą ograniczać funkcjonowanie rynku wewnętrznego, istnieje potrzeba zapewnienia zharmonizowanej ochrony prawnej przed obchodzeniem skutecznych zabezpieczeń technologicznych oraz przeciw zaopatrzeniu w urządzenia i produkty lub usługi służące temu celowi.

Taka ochrona prawna powinna dotyczyć środków technologicznych, które pozwalają skutecznie ograniczyć działania, na które podmioty praw autorskich nie wydały zezwolenia, (...) nieutrudniając jednak normalnego funkcjonowania sprzętu elektronicznego i jego technologicznego rozwoju. (...) **Taka ochrona prawna powinna respektować zasadę proporcjonalności** i nie powinny być zabronione urządzenia lub działania, których istotny handlowy cel i wykorzystanie jest inny, niż obchodzenie ochronnych środków technicznych. **Ochrona ta nie powinna w szczególności stanowić przeszkody dla badań nad kryptografią.**

Ochrona prawna środków technologicznych nie narusza stosowania przepisów krajowych, które mogą zabraniać posiadania do celów prywatnych urządzeń, produktów lub części składowych przeznaczonych do obchodzenia środków technologicznych.

dr Wojciech R. Wiewiórowski



2. Techniczne zabezpieczenia

Techniczne zabezpieczenia (definicja legalna)

Wszelkie technologie, urządzenia lub ich elementy, których przeznaczeniem jest zapobieganie działaniom lub ograniczenie działań umożliwiającym korzystanie z utworów lub artystycznych wykonań z naruszeniem prawa;

Skuteczne techniczne zabezpieczenia (definicja legalna)

Techniczne zabezpieczenia umożliwiające podmiotom uprawnionym kontrolę nad korzystaniem z chronionego utworu lub artystycznego wykonania poprzez zastosowanie kodu dostępu lub mechanizmu zabezpieczenia, w szczególności szyfrowania, zakłócania lub każdej innej transformacji utworu lub artystycznego wykonania lub mechanizmu kontroli zwielokrotniania, które spełniają cel ochronny;

Informacje na temat zarządzania prawami

Informacje identyfikujące utwór, twórcę, podmiot praw autorskich lub informacje o warunkach eksploatacji utworu, o ile zostały one dołączone do egzemplarza utworu lub są przekazywane w związku z jego rozpowszechnianiem, w tym kody identyfikacyjne.

3. Zakaz posiadania w prawie karnym

- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny
- Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii
 - Ustawa z dnia 21 maja 1999 r. o broni i amunicji



3.1. Dlaczego zakaz posiadania

- Cele prewencyjne – zapobieganie zagrożeniom, jakie stwarza nie kontrolowany obrót i kontakt ludzi z określonymi, uznanymi przez ustawodawcę za niebezpieczne, przedmiotami
- Ochrona porządku publicznego
- Bezpieczeństwo
- Dążenie do kontroli



3.2. Czego nie wolno posiadać

Art. 171 § 1 kodeksu karnego

Kto, bez wymaganego zezwolenia lub wbrew jego warunkom, wyrabia, przetwarza, gromadzi, posiada, posługuje się lub handluje substancją lub przyrządem wybuchowym, materiałem radioaktywnym, urządzeniem emitującym promienie jonizujące lub innym przedmiotem lub substancją, która może spowodować niebezpieczeństwo dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

3.2. Czego nie wolno posiadać

Art. 202 § 3 kodeksu karnego

Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub publicznie prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

3.2. Czego nie wolno posiadać

Art. 202 § 4 kodeksu karnego

Kto sprowadza, przechowuje lub posiada treści pornograficzne z udziałem małoletniego poniżej lat 15, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

3.2. Czego nie wolno posiadać

Art. 263 § 2 kodeksu karnego

Kto bez wymaganego zezwolenia posiada broń palną lub amunicję, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

3.2. Czego nie wolno posiadać

Art. 54 ustawy o przeciwdziałaniu narkomanii

Kto wyrabia, posiada, przechowuje, zbywa lub nabywa przyrządy, jeżeli z okoliczności wynika, że służą one lub są przeznaczone do niedozwolonego wytwarzania, przetwarzania lub przerobu środków odurzających lub substancji psychotropowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

3.2. Czego nie wolno posiadać

Art. 62 ustawy o przeciwdziałaniu narkomanii

1. Kto, wbrew przepisom ustawy, **posiada** środki odurzające lub substancje psychotropowe, podlega karze pozbawienia wolności do lat 3.
2. Jeżeli przedmiotem czynu, o którym mowa w ust.1, jest znaczna ilość środków odurzających lub substancji psychotropowych, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
3. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3.2. Czego nie wolno posiadać

Art. 54 ustawy o broni i amunicji

Kto bez wymaganej rejestracji posiada broń pneumatyczną albo zbywa osobie nieuprawnionej broń pneumatyczną albo miotacz gazu o bezwładniającym lub narzędzie albo urządzenie, którego używanie może zagrażać życiu lub zdrowiu, podlega karze aresztu albo grzywny.

4.1. Czego nie może posiadać informatyk

- Art. 118¹.** 1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

4.2. Czego nie może posiadać informatyk

Proponowane brzmienie

Art. 118¹.

1. Kto wytwarza urządzenia, ich komponenty lub programy komputerowe, których jedynym albo głównym przeznaczeniem jest niedozwolone usuwanie lub obchodzenie skutecznych technicznych zabezpieczeń przed odtwarzaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami, ich komponentami lub programami komputerowymi albo reklamuje je w celu sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. **Kto posiada, przechowuje lub wykorzystuje urządzenia, ich komponenty lub programy komputerowe, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.**



5. Czym jest program komputerowy ?

- Prawo polskie nie zawiera dziś jasnej definicji tego czym jest program komputerowy
- Definicja programu komputerowego jest formułowana na potrzeby prawa autorskiego
- Regulacja nakierowana jest jedynie na programy komputerowe, które są jednocześnie utworami w rozumieniu prawa autorskiego
- Dzieło informatyczne ma status utworu, jeśli jest przejawem działalności twórczej o indywidualnym charakterze oraz zostało „ustalone” w jakiegokolwiek formie
- Przykładowo ustawa – Prawo własności przemysłowej posługuje się jednocześnie niedefiniowanymi pojęciami „programu komputerowego” oraz „programu do maszyn cyfrowych”. Ustawodawca posłużył się celowo w art. 28 tej ustawy pojęciem „program do maszyn cyfrowych”, zaś mówiąc w art. 102 ust. 2 o tym, co nie może być wytworem, którego postać może mieć charakter wzoru przemysłowego, równie celowo posłużył się pojęciem programu komputerowego.



5. Czym jest program komputerowy ?

programem komputerowym
jest takie dzieło informatyczne,
które jest przejawem działalności twórczej
o indywidualnym charakterze oraz
zostało „ustalone” w jakiegokolwiek formie

6. Co nakazuje dyrektywa ?

1. Państwa Członkowskie przewidują **stosowną ochronę** prawną przed obchodzeniem skutecznych środków technologicznych przez daną osobę, której znane jest lub w zależności od okoliczności musi być znane to, że zmierza lub ona w tym celu.
2. Państwa Członkowskie przewidują **stosowną ochronę** prawną przed produkcją, przywozem, rozpowszechnianiem, sprzedażą, najmem, reklamą w celach sprzedaży lub najmu lub przed **posiadaniem w celach handlowych** urządzeń, produktów lub części składowych oraz świadczeniem usług, które:
 - a) stanowią przedmiot promocji, reklamy lub sprzedaży w celu obejścia skutecznych środków technologicznych; lub
 - b) posiadają tylko ograniczony, mający handlowe znaczenie cel lub zastosowanie inne niż obejście skutecznych środków technologicznych; lub
 - c) są głównie zaprojektowane, produkowane, dostosowane lub realizowane do celu umożliwienia lub ułatwienia obchodzenia skutecznych środków technologicznych.

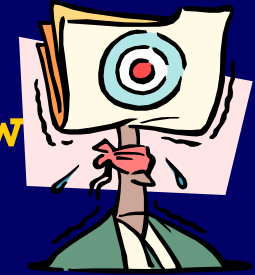
7.Haking



W polskim prawie nie zdefiniowano pojęcia *hakera*

- osoba, która uzyskuje nieuprawniony dostęp do systemu komputerowego lub dokumentu elektronicznego przy pomocy narzędzi informatycznych
 - nowicjusz
 - cyberturysta
 - gracz
 - analityk lub badacz
 - złodziei
 - wandali
 - szpieg

W prawie nie rozróżnia się grup *hakerów*. Działanie niezależnie od pobudek regulowane jest tymi samymi przepisami.



7.1. Haking - Typy psychologiczne sprawców

- **gracze** - *prowadzą swoistą grę z twórcami zabezpieczeń, nie rozpowszechniają wirusów i narzędzi hackerskich, a jedynie tworzą ich prototypy*
- **rookie** - *młodzi programiści sprawdzający swe umiejętności i poszukujący sławy*
- **wandale** - *ich celem jest uszkodzenie systemom*
- **technicy specjaliści** - *wirusy i narzędzia hackerskie służą im do dokonania innych przestępstw niż hacking czy cracking*

7.2. Istota nowelizacji *hackingu* z 2004 r.



Aktualna regulacja zawarta w Kodeksie karnym, którą możemy określić jako „*antyhakerską*”, sprowadza się do przepisów artykułów 267, 268 i 268a

„Art. 267. § 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub **przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie**, podlega (...).

Art. 268. § 1. Kto, nie będąc do tego uprawnionym, **niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji** albo **w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią**, podlega (...)

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, **niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych** albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

7.3. Propozycja nowelizacji z 2008 r.

Projekt zmiany ustawy – Kodeks karny przygotowany
przez Ministerstwo Sprawiedliwości



w tym zakresie powtarza rozwiązania z tzw. Kodeksu Ziobry

Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nie przeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. **Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.**

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem specjalnym.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.



Informatyk w okowach prawa karnego

7.3. Propozycja nowelizacji z 2008 r.

Projekt zmiany ustawy – Kodeks karny przygotowany
przez Ministerstwo Sprawiedliwości



w tym zakresie powtarza rozwiązania z tzw. Kodeksu Ziobry

Z uzasadnienia

Zaproponowano również rozwiązania dotyczące zwalczania przestępstw informatycznych. Penalizacji będą podlegać – zgodnie z projektem – czyny polegające na nielegalnym dostępie do systemu informatycznego, nielegalnej ingerencji w system oraz w dane gromadzone w tym systemie. Przyjęto, że karane będą ponadto czynności takie m.in. jak: nieuprawnione uzyskanie dostępu do informacji nawet bez złamania zabezpieczenia zainstalowanego w komputerze lub systemie czy utrudnienie dostępu do danych komputerowych.

dr Wojciech R. Wiewiórowski

WPiA Uniwersytet Gdański



8. Czego nie wolno posiadać ?

Art. 269 b

Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w [tu lista przestępstw] a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanej w systemie komputerowym lub sieci teleinformatycznej
podlega karze pozbawienia wolności do lat 3.

- spowodowanie niebezpieczeństwa przez *sabotaż komputerowy*
- podsłuch komputerowy
- niszczenie danych,
- sabotaż komputerowy
- zakłócenie pracy sieci



dr Wojciech R. Wiewiórowski

WPIA Uniwersytet Gdański



Informatyk w okowach prawa karnego

9. Niemcy powielają polskie błędy

Ustawa o zmianie ustawy kodeks karny w celu zwalczaniu przestępczości komputerowej
(Bundestag 25 maja 2007 r.)

§ 202a 1. Kto, w sposób nieuprawniony umożliwia (dostarcza) sobie lub innej osobie dostęp do danych, które nie są dla niego przeznaczone i które są w sposób szczególny zabezpieczone przeciw nieuprawnionemu dostępowi, poprzez przewyciężenie zabezpieczeń dostępu,
podlega karze pozbawienia wolności do lat 3 albo karze grzywny

[...]

§ 202 b 1. Ta ustawa służy implementacji konwencji Rady Europy o cyberprzestępczości oraz implementacji decyzji ramowej 2005/222/UE Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. U. UE L 69 s. 67)

2. Kto w sposób nieuprawniony przy użyciu środków technicznych umożliwia sobie albo innej osobie, dostęp do danych dla niego nie przeznaczonych i pochodzących z niepublicznej transmisji danych lub elektromagnetycznej emisji urządzenia służącego do przetwarzania danych,
podlega karze pozbawienia wolności do lat dwóch lub karze grzywny,
jeżeli czyn ten nie podlega na podstawie innych przepisów karze surowszej.

§ 202c 1. Kto czyni przygotowania do popełnienia czynu określonego w § 202 a lub § 202 b, w taki sposób, iż:

(1) hasła lub inne kody bezpieczeństwa, które umożliwiają dostęp do danych (§ 202a ust. 2) lub

(2) programy komputerowe, których celem jest popełnienie takiego czynu, **wytwarza, zdobywa dla siebie lub innej osoby, sprzedaje, przekazuje innej osobie rozpowszechnia lub umożliwia w inny sposób do nich dostęp,**

podlega karze pozbawienia wolności do roku lub karze grzywny.

Informatyk w okowach prawa karnego

10. Konwencja o cyberprzestępczości

Tytuł 1 Przepisy przeciwko poufności, integralności i dostępności danych informatycznych i systemów

Artykuł 2 **Nielegalny dostęp**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, **umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego**. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym.

Artykuł 3 **Nielegalne przechwytywanie danych**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, **umyślnego, bezprawnego przechwytywania za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne**. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym.

Informatyk w okowach prawa karnego

10. Konwencja o cyberprzestępczości

Artykuł 4 Naruszenie integralności danych

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, **umyślnego, bezprawnego niszczenia, wykasowywania, uszkodzania, dokonywania zmian lub usuwania danych informatycznych.**
2. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie 1 musi skutkować poważną szkodą.

Artykuł 5 Naruszenie integralności systemu

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, **umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkodzanie, dokonywanie zmian lub usuwanie danych informatycznych.**

Informatyk w okowach prawa karnego

10. Konwencja o cyberprzestępczości

Artykuł 6 Niewłaściwe użycie urządzeń

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych:

a. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:

- **urządzenia, w tym także programu komputerowego**, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregośkolwiek z przestępstw określonych zgodnie z artykułami 2-5;

- **hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna,**

z zamiarem wykorzystania dla celów popełnienia któregośkolwiek z przestępstw określonych zgodnie z artykułami 2-5; oraz

b. posiadania jednostki wymienionej powyżej w punktach a. i. lub ii. z zamiarem wykorzystania w celu popełnienia któregośkolwiek z przestępstw określonych zgodnie z artykułami 2-5.

Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek.

Informatyk w okowach prawa karnego

10. Konwencja o cyberprzestępczości

Ale Konwencja mówi też:

Niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcie do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego.

Każda Strona może zastrzec sobie prawo do niestosowania ustępu 1 niniejszego artykułu, pod warunkiem, że zastrzeżenie to nie dotyczy sprzedaży, dystrybucji lub innego udostępniania jednostek wymienionych w ustępie 1.a.ii.

11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r.
w sprawie ataków na systemy informatyczne

Unia Europejska uznała, że istnieje potrzeba ustanowienia przez Państwa Członkowskie sankcji za ataki na systemy informatyczne. Przewidziane sankcje powinny być skuteczne, proporcjonalne i odstraszające

Ponieważ cele niniejszej decyzji ramowej, czyli zapewnienie, że we wszystkich Państwach Członkowskich ataki na systemy informatyczne są zagrożone skutecznymi, proporcjonalnymi i odstraszającymi sankcjami karnymi oraz usprawnianie i zachęcanie do współpracy sądowej poprzez usuwanie potencjalnych przeszkód, nie mogą być w sposób wystarczający osiągnięte przez Państwa Członkowskie w związku z tym, że zasady muszą być wspólne i kompatybilne, natomiast możliwe jest lepsze osiągnięcie tych celów na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu WE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza decyzja ramowa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r.
w sprawie ataków na systemy informatyczne

Najpierw dwie definicje:

a) „system informatyczny”

wszelkie urządzenia lub grupa połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania;

b) „dane komputerowe”

wszelkie przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system;

11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r.
w sprawie ataków na systemy informatyczne

Artykuł 2

Nielegalny dostęp do systemów informatycznych

1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślny bezprawny dostęp do całości lub części systemu informatycznego jest karalny jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.
2. Każde Państwo Członkowskie może zdecydować, że zachowanie, o którym mowa w ust. 1 jest objęte oskarżeniem jedynie w przypadkach, kiedy przestępstwo popełniane jest z naruszeniem zabezpieczenia.

**11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r.
w sprawie ataków na systemy informatyczne**

Artykuł 3 **Nielegalna ingerencja w system**

Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkodzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych jest karalne jako przestępstwo, kiedy dokonane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 4 **Nielegalna ingerencja w dane**

Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne bezprawne usunięcie, uszkodzenie, pogorszenie, zmiana, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym jest karane jako przestępstwo, kiedy dokonywane jest bezprawnie,
przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r.
w sprawie ataków na systemy informatyczne

Artykuł 5 **Kierowanie, pomaganie i podżeganie
oraz usiłowanie**

1. Każde Państwo Członkowskie zapewnia, że kierowanie, pomaganie i podżeganie do przestępstw, o których mowa w art. 2, 3 i 4, jest karane jak przestępstwo.
2. Każde Państwo Członkowskie zapewnia, że usiłowanie popełnienia przestępstw, o których mowa w art. 2, 3 i 4, jest karane jak przestępstwo.
3. Każde Państwo Członkowskie może zdecydować o niestosowaniu ustępu 2 do przestępstw, o których mowa w art. 2.

Informatyk w okowach prawa karnego

11. Decyzja ramowa 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne

Ale decyzja ramowa mówi również:

Istnieje potrzeba uniknięcia nadmiernej kryminalizacji, szczególnie w przypadkach mniejszej wagi, jak również potrzeba uniknięcia kryminalizacji posiadaczy praw i osób upoważnionych.

12. Czego nie wolno posiadać ?



Informatyk w okowach prawa karnego

Szkoła Hakerów - interaktywny zestaw edukacyjny - haker - hack - hacker - hacking [26-137] - Microsoft Internet Explorer

Szkoła Hakerów - interaktywny zestaw edukacyjny - haker - hack - hacker - hacking [26-137] - Microsoft Internet Explorer

Plik Edycja Widok Ulubione Narzędzia Pomoc

Wstecz Wyszukaj Ulubione

Adres Przejdź Łącz

Zamów Limitowaną Edycję Zestawu Szkoleniowego Szkoły Hakerów -- Oferta Ważna do Wyczerpania Zapasów!

Tak! Zamawiam zestaw w cenie **137 zł**, warty co najmniej 689 zł, **oszczędzam zatem co najmniej 552 zł!** Otrzymam zestaw Szkoły Hakerów, który zawiera:

- **426-stronnicowy Podręcznik szkoleniowy Szkoła Hakerów**
- **1 płytę DVD z 217 minutami Filmów Szkoleniowych**
- **1 płytę CD ze Szkoleniowym Systemem Operacyjnym, który uruchamia się z napędu bez konieczności instalacji**
- **Możliwość wzięcia udziału w teście i otrzymania Certyfikatu Ukończenia Szkolenia z Zakresu Bezpieczeństwa Systemów Komputerowych**
- **Dostęp do zamkniętego Forum Dyskusyjnego Hakerów, gdzie udzielają się autorzy szkolenia, gdzie wymienisz się wiedzą z innymi uczestnikami kursu**
- **Aż 5 konsultacji e-mail z autorami szkolenia - hakerami, ekspertami ds. bezpieczeństwa systemów komputerowych**

TAK! Wiem, że mogę **wypróbować zestaw Szkoły Hakerów BEZ RYZYKA** z Twoją 100% bez-zbędnych-pytań, 30 dniową **GWARANCJĄ** zwrotu pieniędzy.

Aby zamówić, wypełnij poniższy formularz zamówienia. Pamiętaj, by stosować polskie znaki diakrytyczne (ąęśóóźź).

dr Wojciech R. Wiewiórowski

WPIA Uniwersytet Gdański

Informatyk w okowach prawa karnego

http://www.hakerczat.prv.pl/programy/lamacze.html - Microsoft Internet Explorer

Plik Edycja Widok Ulubione Narzędzia Pomoc



Adres



Oficjalny serwis internetowy [czatu #haker na Onet.pl](#)

MENU	TREŚĆ	INFORMACJE
<p>Strona główna</p> <p>Artykuły</p> <p>Różności</p> <p>Sekcje tematyczne</p> <p>Download</p> <p>Forum dyskusyjne</p> <p>Kontakt i linkownia</p> <p>Napisz do nas</p>	<h2>Lamacze haseł.</h2> <p>MD5Search v1.5 Cracker hashy md5 korzystający z 23 crackerskich serwisów online, duża szybkość, plik 246 kB, freeware, system Windows, wygląd programu: screen, Opis na stronie domowej autora projektu: http://mass.uk.to/</p> <p>PassTool 5.0 Dekoder haseł z kilku popularniejszych programów tj. Internet Explorer, Outlook Express, Total Commander, Mozilla Firefox, Gadu-Gadu, Klucze MS Office i Windows, system Windows, freeware, więcej na stronie domowej: http://mass.uk.to/</p> <p>Quick MD5 Decoder v1.4 Dekoder hashy md5 korzystający z 18 crackerskich serwisów online, system Windows, freeware, więcej na stronie domowej: http://mass.uk.to/</p> <p>Słownik angielski Słowniki do łamaczy haseł (angielski i 2 polskie) Słownik polski mały Słownik polski duży Słowniki pochodzą ze strony: http://www.hasla.kom.pl/</p> <p>Quick MD5 Password Decoder 1.3 Prosty i szybki program do dekodowania haseł zahash'owanych w MD5, przy użyciu 7 serwisów crackerskich, metoda słownikowa bądź brute force (w zależności od serwisu - kolejowanie), system Windows, strona domowa: http://www.e-mass.org/</p> <p>PicoZipRecovery Tool Wyciąga hasła z plików .zip, używa słowników, na stronie domowej są słowniki w różnych językach, system Windows 95/98/ME/NT/2000/XP, strona domowa: http://www.picozip.com/prt/</p>	<p>#czat HAKER#</p> <p>Wprost</p> <p>Dz.Internautów</p> <p>I D G</p> <p>e Gospodarka</p> <p>Bugtraq PL</p> <p>Hacking Top</p>

dr Wojciech R. Wiewiórowski

WPIA Uniwersytet Gdański

Informatyk w okowach prawa karnego

The screenshot shows a Microsoft Internet Explorer browser window displaying the IDG.pl website. The address bar shows the URL 'Bezpieczeństwo\Łamacze haseł: Programy'. The website header includes a search bar with 'download linux' entered, a navigation menu with categories like 'Aparaty', 'Biznes', 'Bezpieczeństwo', 'Domeny', 'DVD', 'Gry', 'HDTV', 'Mobile', and 'Notebooki', and a calendar for April 2007. The main content area is titled 'BEZPIECZEŃSTWO\ŁAMACZE HASEŁ' and lists two programs: 'John the Ripper 1.6' (Freeware) and 'Crack 5.0a' (Freeware). The left sidebar contains navigation links for 'MOJE KONTO', 'WINDOWS', 'LINUX', 'MAC OS', 'GRY', and 'SONDA'. The right sidebar features promotional banners for 'Bezpłatny newsletter', 'iDesk - komunikator i nie tylko', and 'F-PROT Antivirus'.

dr Wojciech R. Wiewiórowski

WPIA Uniwersytet Gdański

13. Jak można stać się przestępcą ?

**Myślą, mową, uczynkiem
i zaniechaniem**



Informatyk w okowach prawa karnego

... tym samym ...

Każdy szanujący się administrator sieci, chcący chronić poprawnie zasoby systemu, którym administruje...

... powinien posiadać i używać hakerskiego oprogramowania ...

... co powoduje, że na mocy art. 269 b k.k. ...

... podlega karze pozbawienia wolności do lat 3.



**Każdy administrator sieci jest więc
permanentnym przestępcą**

co było do udowodnienia

dr Wojciech R. Wiewiórowski

WPiA Uniwersytet Gdański



14. ORGANIZACJA PRZESTĘPCZA

Art. 258 k.k.

- Związek przestępny
- Zorganizowana grupa przestępcza

14. ORGANIZACJA PRZESTĘPCZA

Art. 258 kodeksu karnego

§ 1. Kto bierze udział w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli grupa albo związek określone w § 1 mają charakter zbrojny albo mają na celu popełnienie przestępstwa o charakterze terrorystycznym, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto grupę albo związek określone w § 1 w tym mające charakter zbrojny zakłada lub taką grupę albo związkiem kieruje, podlega karze pozbawienia wolności od roku do lat 10.

§ 4. Kto grupę albo związek mające na celu popełnienie przestępstwa o charakterze terrorystycznym zakłada lub taką grupę lub związkiem kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.



14. Związek przestępny

- co najmniej 3 osoby
- względnie stała struktura organizacyjna
- posiada wspólny cel, program działania, formy współdziałania, podział funkcji i zadań, określone kierownictwo i ustalone zasady członkostwa

15. Zorganizowana grupa przestępcza

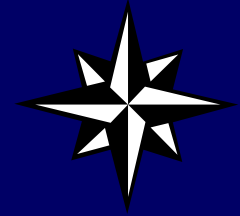
- nie musi mieć długofalowego programu działania
- nie jest konieczne posiadanie ustalonych zasad członkostwa (przynależności)
- mniejszy stopień zorganizowania



16. Haking a ochrona korespondencji



- Art. 267 wzorowany art. 172 Kk z 1969 r., dotyczącym ochrony korespondencji
- Nie bierze się pod uwagę faktu, że cel sprawcy naruszenia nietykalności korespondencji i cel *haker*a jest z zasady różny.
- Dodatkowy problem stanowi, udowodnienie *hakerowi*, że z informacją na *zhakowanym* nośniku się zapoznał. Nawet jeśli wykradł dane w wielu przypadkach nie mamy możliwości stwierdzenia, czy skradzione pliki kiedykolwiek otworzył.
- Możliwość pociągnięcia do odpowiedzialności karnej *haker*a pozostawia art. 268 § 1 (uzupełniany przez § 2) oraz art. 268a § 1 <iluzoryczna możliwość>
 - karalność „zmiany” informacji jest już znaczącym zagrożeniem dla *haker*a.



17. Kto, co i jak może zakłócać ?

Pomieszanie pojęć w treści przepisów artykułu 268a §§ 1 i 2 z jednej strony i artykułu 269a.

Jeśli wg określenia konwencyjnego **praca systemu komputerowego polega na przetwarzaniu gromadzeniu lub przekazywaniu danych**, to nie bardzo jasne jest, co miał na myśli polski ustawodawca, odróżniając „istotne zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia i przekazywania danych” (Art. 268a § 1) od „istotnego zakłócenia pracy systemu komputerowego” (Art. 269a).

O tym, jak poważnym błędem jest takie pomieszanie pojęć, przekonujemy się, gdy zwrócimy uwagę na różne sankcje występujące w wyżej wymienionych przepisach.



Informatyk w okowach prawa karnego



I tym optymistycznym akcentem
kończąc
zachęcamy do zadawania pytań

dr Wojciech R. Wiewiórowski

ul. J.Bażyńskiego 6, pok 1032
80-952 Gdańsk
+48-58-523 29 76

wojciech.wiewiorowski@mswia.gov.pl

dr Wojciech R. Wiewiórowski

Wydział Prawa i Administracji,
Uniwersytet Gdański

