# Bezpieczeństwo systemów i sieci komputerowych

**dr inż. Mirosław Mazurek**

Zakład Systemów Złożonych
**Bud. F, pok. 305, tel. 17 865 11 04**

# Podstawowe definicje

**System** (stgr. *σύστημα systema* – rzecz złożona) – obiekt fizyczny lub abstrakcyjny, w którym można wyodrębnić zespół lub zespoły elementów wzajemnie powiązanych w układy, realizujących jako całość funkcję nadrzędną lub zbiór takich funkcji (funkcjonalność).

Elementy przynależące do jednego systemu nie mogą jednak stanowić jednocześnie elementów przynależnych do innego systemu.

Za kryterium podziału przyjmując wymienialność elementów systemów, w trakcie ich działania systemy dzieli się na:
otwarte np. organizmy biologiczne,
domknięte np. maszyny informacyjne typu komputery,
zamknięte np. maszyny energetyczne typu prądnica.

# Podstawowe definicje

**System informatyczny** to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej.

Obejmuje:

sprzęt – komputery, urządzenia służące do przechowywania danych, do komunikacji między sprzętowymi elementami systemu oraz ludźmi a komputerami, do odbierania danych ze świata zewnętrznego – *nie od ludzi* (na przykład czujniki elektroniczne, kamery, skanery), do przetwarzania danych niebędące komputerami

oprogramowanie

zasoby osobowe

elementy organizacyjne – czyli procedury (procedury organizacyjne – termin z zarządzania) korzystania z systemu informatycznego, instrukcje robocze itp.

elementy informacyjne; bazy wiedzy – ontologie dziedziny/dziedzin, w których używany jest system informatyczny – na przykład podręcznik księgowania w wypadku systemu finansowo-księgowego

# Podstawowe definicje

**Bezpieczeństwo**

– zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności.

**Poufność** – ochrona przechowywanych lub transmitowanych danych przed atakiem włamywaczy w celu zapobiegania ujawnieniu ich treści.

**Integralność** – funkcja bezpieczeństwa polegająca na tym, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.

**Dostępność** – cecha informacji stanowiąca, że tylko upoważnione osoby mogą z niej skorzystać w danym miejscu i czasie. Jedna z podstawowych właściwości bezpieczeństwa informacji.

# Bezpieczny system komputerowy

**Bezpieczny system komputerowy** jest wyidealizowanym urządzeniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela.

**Czy istnieje taki system?**

W praktyce budowa skomplikowanego systemu spełniającego te założenia jest z reguły niemożliwa.

Powody:

- ryzyko wystąpienia prozaicznych usterek i błędów,

- trudność określenia i sformalizowania często sprzecznych oczekiwań projektanta oprogramowania, programisty, prawowitego właściciela systemu, posiadacza przetwarzanych danych, czy w końcu użytkownika końcowego.

- trudność określenia, że dany program spełnia sformalizowane oczekiwania.

# Normy dotyczące bezpieczeństwa informacji

**PN-I-13335-1: 1999**
„Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych”

**ISO/IEC TR 13335-2:2003**
„Zarządzanie i planowanie bezpieczeństwa systemów informatycznych”

**ISO/IEC TR 13335-3:2003**
„Techniki zarządzania bezpieczeństwem systemów informatycznych”

**PN ISO/IEC 17799:2003**
„Praktyczne zasady zarządzania bezpieczeństwem informacji”

**PN –I- 07799-2:2005**
„Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne stosowania” (przyjęta do ustanowienia we wrześniu 2004; identyczna z BS 7799-2:2002)

# Sposoby walki z zagrożeniami bezpieczeństwa

- **skuteczne zapobieganie powstawaniu usterek**

- **budowanie systemów w sposób, który ogranicza ewentualne problemy wynikające z naruszenia zabezpieczeń lub niepożądanej aktywności uprawnionego użytkownika**

- **zredukowanie ryzyka pomyłek przy tworzeniu oprogramowania**

    - Odpowiednia budowa protokołów i interfejsów

    - Wybór metod programistycznych

    - Testowanie jakości aplikacji
        - Przegląd kodu źródłowego
        - Testy typu czarna skrzynka
        - Testy siłowe

# Zarządzanie bezpieczeństwem

- Ograniczanie interakcji

- Ograniczanie uprawnień

- Rozliczalność i nadzór operacyjny

**[*SPAM*] Twoje Konto E-mail Zostalo Zaplanowane Na Zawieszenie**

Email Administrator <m.kasztura.gops@liszki.pl>

Wysłano: czw. 26.10.2017 04:17

Do: Recipients

Twoje konto e-mail zostało zaplanowane na zawieszenie.

Co się stało?

* Z Twojej skrzynki pocztowej dostrzegamy pewne nieprawidłowości.
* Nieautoryzowany dostęp do Twojego adresu e-mail z adresu IP znajdującego się na czarnej liście.
* Na Twoim koncie brakuje niektórych informacji.
* Nielegalna próba użycia konta w innym miejscu

Musisz się zgodzić z tym LINKem < KLIKNIJ TUTAJ > i wypełnić odpowiednie informacje, a to nie spowoduje zawieszenia konta.

Dziękuję za współpracę

ZESPOŁY BEZPIECZEŃSTWA WEB ADMIN

# Aspekt prawny

## Sabotaż informacji i systemu informatycznego

- Pod karę tą podlegają również inne działania mające na celu **uniemożliwienie lub znaczne utrudnienie osobie uprawnionej zapoznanie się z informacją**. Jeżeli wymienione przestępstwa dotyczą zapisu informacji w formie elektronicznej, podlegają karze nawet do 3 lat. Artykuł 268a wskazuje, że karą pozbawienia wolności do **3 lat**, objęte są również przestępstwa polegające na **nieuprawnionym niszczeniu, uszkodzeniu, zmianie lub utrudnieniu dostępu do danych informatycznych, obejmujące również zakłócanie automatycznego przetwarzania, gromadzenia lub przekazywania danych.**

- Wymienione kary dotyczą działań, których efektem nie ma dużych szkód majątkowych. W przypadku wyrządzenia **znacznych szkód majątkowych** kara pozbawienia wolności wynosi od **3 miesięcy** nawet do **5 lat**. **Administrator informacji musi być świadomy** dokonywanych przestępstw w swoim systemie, bowiem ściganie wymienionych przestępstw następuje na wniosek pokrzywdzonego. Ważnym jest zatem wyposażenie systemu przetwarzania danych w narzędzia identyfikacji zagrożeń i wykrywania dokonanych zamian w zapisach danych.

- **Przestępstwo polegające na uszkodzeniu, usunięciu lub zmianie zapisu istotnej informacji** jest zidentyfikowane w artykule 268 Kodeksu Karnego i podlega karze pozbawienia wolności do **2 lat**.

- **Zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej poprzez transmisję, modyfikację lub utrudnienie dostępu do danych informatycznych** podlega karze pozbawienia wolności od **3 miesięcy** do **5 lat**.

# Aspekt prawny

## Przestępstwa przeciwko organom Państwa

Przestępstwa dotyczące danych informatycznych gromadzonych w instytucjach państwowych opisane są w artykule 269 Kodeksu Karnego.

Zabronione jest:

- niszczenie,
- uszkadzanie,
- usuwanie
- zmiana danych informatycznych

o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

Artykuł ten opisuje również jako czyny zabronione zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych i określa karę pozbawienia wolności **od 6 miesięcy do lat 8.** Zapisy tego artykułu dotyczą informacji zapisanych i przetwarzanych w formie elektronicznej jak i poza takim systemem.

# Aspekt prawny

## Nieuprawnione uzyskanie informacji

Zgodnie z artykułem 267 Kodeksu Karnego **uzyskiwanie informacji przez osobę nieuprawnioną lub informacji nie przeznaczonych dla niej** podlega karom grzywny, ograniczenia wolności lub pozbawienia wolności do 2 lat. **Karalny jest czyn odczytania zabezpieczonych danych** jak również sam **czyn uzyskania dostępu do systemu informatycznego bez faktycznego odczytania danych**. Tej samej karze podlega osoba, która dokonuje podsłuchu systemu uzyskując tym samym informacje do których nie jest uprawniony. Ujawnienie tak uzyskanych danych jest również karalne nawet pozbawieniem wolności **do 2 lat**. Ściganie przestępstwa następuje na wniosek pokrzywdzonego. Ważne jest zatem, aby administrator danych miał możliwość wykrycia włamania i oceny jego rozmiarów.

Ochrona korespondencji elektronicznej realizowana jest także przez prawo cywilne, szczególnie gdy zaistniały określone skutki. Artykuł 25 Kodeksu Cywilnego pozwala na żądanie usunięcia skutków, a jeśli zaistniała szkoda majątkowa, poszkodowany może żądać jej naprawienia w ramach przepisów ogólnych. W zakresie odpowiedzialności za czyny niedozwolone art. 415 stanowi: Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.

Omawiany problem w świetle prawa cywilnego dotyczy także ochrony nadawcy korespondencji. Może tu zachodzić np. przesłanie korespondencji bez zabezpieczenia jej treści (odpowiednimi kodami kryptograficznymi w wypadku poczty elektronicznej).

# Aspekt prawny

## Ułatwianie popełnienia przestępstwa

Umożliwianie popełnienia przestępstwa polegające na:

- tworzeniu,
- rozprzestrzenianiu
- lub pozyskaniu urządzenia lub programu komputerowego przystosowanego do popełnienia przestępstwa na informacji

podlega karze pozbawienia wolności do **3 lat** z artykułu 269b Kodeksu Karnego.

Karalne jest również:
- rozpowszechnianie haseł komputerowych,
- kodów dostępów umożliwiających dostęp do informacji gromadzonych w systemie komputerowym.

W przypadku skazania za powyższe przestępstwa, sąd orzeka przepadek przedmiotów użytych w przestępstwie. Może to stanowić duże zagrożenie dla firmy jeżeli przestępstwa dokonuje pracownik z firmowego komputera. Bardzo ważnym w takiej sytuacji jest częste przeprowadzanie audytu oprogramowania zainstalowanego na komputerach oraz zainstalowanie w sieci narzędzi pomagających wykryć niepożądane oprogramowanie lub urządzenia.

# Aspekt prawny

## Legalność oprogramowania

Przywłaszczenie programu komputerowego bez zgody osoby uprawnionej w szczególności twórcy lub właściciela programu, jest ścigane z artykułu 278.

Karą za to działanie jest kara pozbawienia wolności od **3 miesięcy** do **5 lat**.

Ponadto, zgodnie z artykułem 18 Kodeksu Karnego za kradzież oprogramowania odpowiada **nie tylko sprawca, ale również osoba ułatwiająca dokonanie tego czynu**. Z tego powodu kierownictwo oraz administrator systemu komputerowego są odpowiedzialni za legalność zainstalowanego oprogramowania na komputerach. Utrzymanie takiej odpowiedzialności osobom nie mającym praktycznej kontroli nad instalowanym oprogramowaniem jest dużym nadwyrężeniem obowiązków administratora. Zadanie to można z pełnym powodzeniem przekazać użytkownikom komputerów, czyniąc każdego z osobna odpowiedzialnym za dodatkowe oprogramowanie, które instaluje na komputerze.

# Aspekt prawny

## Treści nielegalne

Treści nielegalne to:

- treści pornograficzne z udziałem małoletniego poniżej 15-go roku życia,

- treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem (art. 202 Kodeksu Karnego),

- treści propagujące publicznie faszystowski lub inny totalitarny ustrój państwa lub nawołujące do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (art. 256 Kodeksu Karnego),

- treści publicznie znieważające grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości (art. 257 Kodeksu Karnego).

Posługiwanie się treściami nielegalnymi podlegać może karze pozbawienia wolności nawet **do 8 lat.** Ponadto Sąd może orzec **przepadek narzędzi lub innych przedmiotów,** które służyły lub były przeznaczone do popełnienia przestępstw z treściami nielegalnymi. Ważnym jest zatem stały monitoring ruchu sieciowego i kontrola odwiedzanych przez użytkowników systemu witryn internetowych.