PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Ewa Staniewska, Justyna Żywiołek
Politechnika Częstochowska,
ul. Armii Krajowej 19, 42-200 Częstochowa; e-mail: staniew@wip.pcz.pl

NARZĘDZIA I TECHNOLOGIE OCHRONY DANYCH

Streszczenie. Informacja jako największe dobro każdej instytucji powinna podlegać ochronie przed niepowołanym dostępem, zniszczeniem lub nieautoryzowaną zmianą. W artykule przedstawiono wybrane aspekty bezpieczeństwa, a w szczególności typy zagrożeń oraz metody ochrony danych.

Słowa kluczowe: bezpieczeństwo danych, narzędzia ochrony danych.

Wstęp

W chwili obecnej jesteśmy świadkami dynamicznego rozwoju informatyki. Osiągnięcia informatyczne są stosowane powszechnie w każdej dziedzinie życia, a szczególnie istotnym obszarem ich zastosowania jest gromadzenie i przetwarzanie nieograniczonej liczny informacji. Informacja stanowi jeden z najbardziej strategicznych zasobów gospodarczych, naukowych i kulturowych.

Popularnym stało się stwierdzenie „kto ma informacje, ten ma pieniądze i władzę". Informacja nie tylko jest gromadzona w postaci ogromnych baz danych lub baz wiedzy, ale przede wszystkim jest przetwarzana. Informacje podlegają szczegółowym analizom badawczym przez kadry zarządzające przedsiębiorstwem. Każda instytucja wykorzystuje nośniki pamięci masowej do przechowywania danych. Dane są również przesyłane z (i do) różnych jednostek. Sposoby przesyłania danych są ciągle analizowane pod kątem bezpieczeństwa. Nowoczesne systemy teleinformatyczne w znacznym stopniu ułatwiają przesyłanie, dystrybucję, wymianę i przetwarzanie danych. Zwiększanie szybkości przekazywania danych o zasięgu globalnym pozwala na generowanie oszczędności nie tylko czasowych, ale również ekonomicznych. Stale rosnący poziom rozwoju sieci teleinformatycznych skutecznie podnosi bezpieczeństwo transmitowanych danych, co dzisiaj staje się bardzo istotne, a momentami wręcz niezbędne do właściwego i bezpiecznego funkcjonowania przekazu. Popularność

przesyłania informacji za pomocą sieci komputerowych poza niewątpliwymi korzyściami, niesie za sobą również wiele niebezpieczeństw, dając możliwości nadużyć, często prowadzących do przestępstw. Dane muszą być chronione zawsze, nie tylko podczas ich przesyłania, ale również i przede wszystkim podczas ich przechowywania.

Aspekty ochrony

Zapewnienie bezpieczeństwa danych polega na ich ochronie, czyli zagwarantowaniu dostępu tylko uprawnionym użytkownikom i zabronieniu dostępu nieuprawnionym, a także na zabezpieczeniu przed przypadkowym lub umyślnym ujawnieniem, aktualizacją lub zniszczeniem [8]. Wyróżniane są cztery podstawowe aspekty bezpieczeństwa:

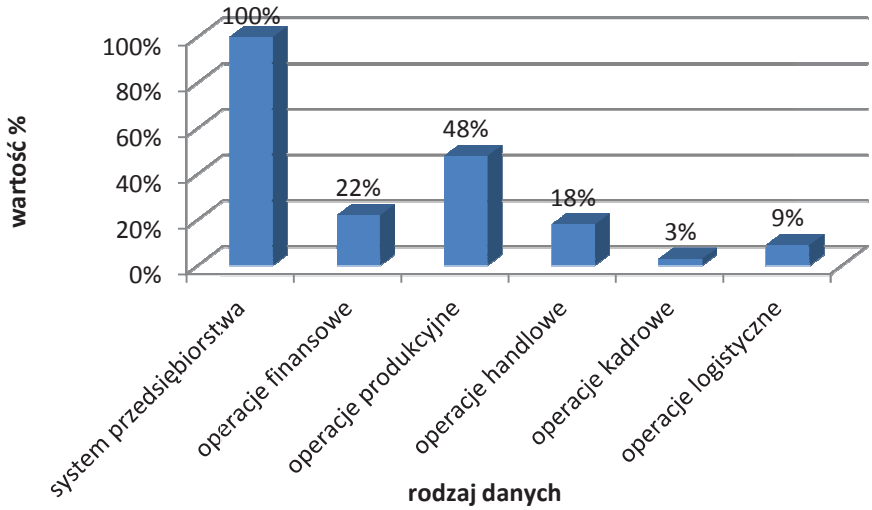
- poufność,
- integralność,
- dostępność,
- spójność.

Poufność danych jest rozumiana jako brak dostępu do danych dla użytkowników oraz aplikacji, które nie są uprawnione do odczytywania jej klauzul bezpieczeństwa w postaci: ściśle tajne, tajne, poufne nadaje się danym newralgicznym z punktu widzenia instytucji. Naruszenie ich poufności wiązałoby się z dużymi kosztami oraz znacznym ryzykiem z punku widzenia funkcjonowania instytucji.

Integralność danych oznacza pewność, że dane nie zostały podmienione, zniekształcone lub zmodyfikowane bez wiedzy ich właściciela. Stan danych pozostaje zgodny ze stanem wymaganym i oczekiwanym przez adresata, do którego są przesyłane. Naruszenie integralności następuje przy nieupoważnionym dostępie, potknięciach i zaniedbaniach użytkowników uprawnionych, nieposiadających odpowiedniego przygotowania lub przeszkolenia. Mogą również być spowodowane awariami sprzętu, zakłóceniami transmisji, błędami w oprogramowaniu lub wirusami. W systemach informatycznych integralność danych powinna być zapewniona podczas ich przechowywania, przetwarzania i przesyłania.

Dostępność danych polega na stworzeniu możliwości ciągłego korzystania z danych dla wszystkich upoważnionych użytkowników. Może ją naruszyć nieupoważniony użytkownik lub upoważniony – przez nieświadome działania. Dostępność może być ograniczona również przez awarie, zakłócenia w transmisji, błędy oprogramowania oraz przeciążenia sieci. W systemach informatycznych główny nacisk kładzie się na zwiększenie dostępności infrastruktury informatycznej, co pozwala optymalizować koszty braku dostępu. Poziom kosz-

tów braku dostepu do systemu informatycznego przez godzinę przedstawia rysunek 1.



Rys. 1. Koszty braku dostępu do systemu informatycznego w przedsiębiorstwie
Źródło: opracowanie własne na podstawie danych GUS.

Dostępność na niskim poziomie powoduje generowanie kosztów związanych z każdą godziną przestoju. W zależności od instytucji, przestoje sięgają od kilkunastu tysięcy do wielu milionów złotych.

Ochrona danych

Spójność dotyczy danych gromadzonych w bazie danych. Wszelkie zmiany w bazie danych stanowią proces dyskretny. Wprowadzane, aktualizowane i usuwane informacje muszą spełniać warunki narzucone na dane podczas definicji bazy danych tak, by baza była zgodna z rzeczywistością. W każdym momencie baza danych znajduje się w określonym stanie. Stan nazywany jest spójnym, jeżeli wszystkie wartości, które zawiera baza danych w tym stanie, mogą zaistnieć w świecie rzeczywistym. Warunki spójności mogą być dynamiczne lub statyczne. Warunki dynamiczne różnią się od statycznych tym, że pamiętają poprzedni stan. Zachodzenie warunków spójności zapewnia poprawność bazy danych. Naruszenie spójności danych następuje w wyniku niepoprawnych operacji, niewłaściwej synchronizacji działań współbieżnych lub w wyniku awarii systemu [3].

Przez bezpieczeństwo informacji należy rozumieć również zachowanie rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Rozliczalność polega na zapewnieniu, że określone działania użytkownika mogą być przypisane w sposób jednoznaczny tylko jemu. Inaczej mówiąc, brana jest pod uwagę odpowiedzialność za wykorzystanie systemu informacyjnego.

Autentyczność dotyczy użytkowników, procesów, i informacji i polega na sprawdzaniu tożsamości podmiotów i prawdziwości zasobów.

Niezaprzeczalność oznacza brak możliwości zaprzeczenia swego uczestnictwa w całości lub w części danych przez jeden z podmiotów uczestniczących w tej wymianie.

Niezawodność gwarantuje spójność danych i systemu oraz oczekiwane jego zachowanie i spodziewane wyniki.

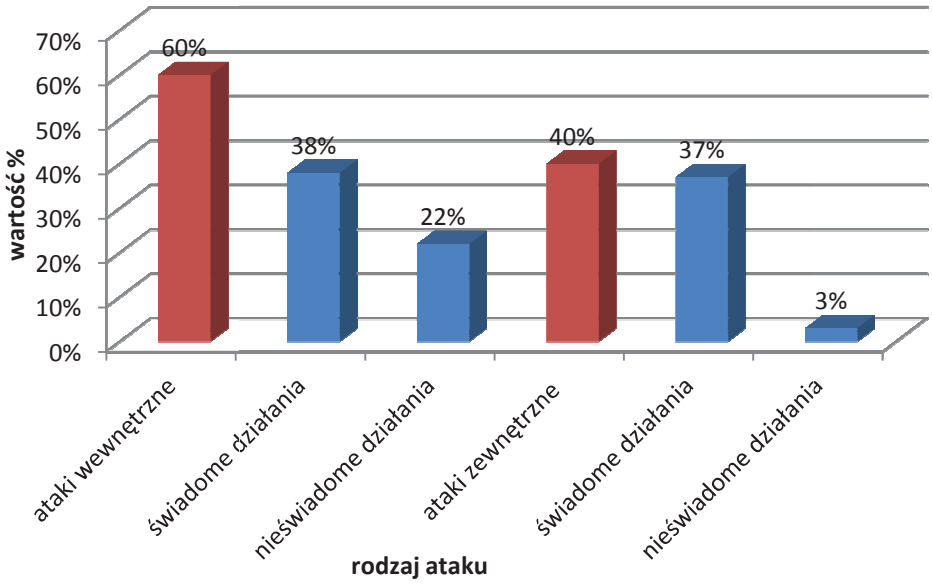
Typy zagrożeń danych

Zagrożenia można podzielić na dwie kategorie: zagrożenia niezależne od człowieka oraz będące celowym lub przypadkowym działaniem człowieka. Do zagrożeń niezależnych od człowieka należą: awarie sprzętu komputerowego, zaniki zasilania, pożary, powodzie, trzęsienia ziemi, zewnętrzne pola elektromagnetyczne. Nieprawidłowe działanie sprzętu komputerowego wynika z wad produkcyjnych, błędów projektowych oraz błędów wynikających z podłączenia sprzętu do sieci, a także awarii związanych z nieodpowiednim środowiskiem zewnętrznym [8]. Często duża wilgotność, drgania, zbyt niska lub wysoka temperatura powodują występowanie awarii sprzętu. Jako sprzęt rozumiemy zestaw komputerowy, którego najbardziej newralgicznym elementem jest pamięć. Postęp naukowo-techniczny dokonujący się w dziedzinie elektroniki cyfrowej prowadzi do automatyzacji procesów produkcji. Sprawdzanie poprawności staje się nieodzownym elementem nie tylko fazy produkcji, lecz również eksploatacji. Z roku na rok przybywa zastosowań układów pamięci, których uszkodzenie może mieć poważne skutki, w zależności od roli systemu, od niezadowolenia potencjalnego użytkownika, poprzez aspekty ekonomiczne, do zagrożenia bezpieczeństwa danych lub ludzi. Wszystko to powoduje wzrost trwałości produkowanych obecnie nośników danych oraz zastosowanie wyższej klasy testów pamięci w trakcie eksploatacji, pozwalające na detekcję uszkodzeń i zamian uszkodzonych komórek poprawnie działającymi. Następuje ogólne zmniejszanie awaryjności sprzętu komputerowego.

Czynnik ludzki jest zawsze najsłabszym ogniwem w systemie bezpieczeństwa. Włamania, podsłuchy, niszczenie danych, wprowadzanie wirusów lub celowe zaniedbywanie swoich obowiązków powoduje obniżenie poziomu bezpieczeństwa. Zagrożenia mogą pochodzić od nieupoważnionych lub upoważnionych użytkowników. Nieupoważnieni użytkownicy muszą znaleźć słabe

strony bezpieczeństwa, oszukać systemy wykrywania intruzów. Dokonują zwykle jednorazowego ataku w celu zmodyfikowania lub zniszczenia określonych danych albo ściągnięcia całej bazy danych.

Użytkownicy upoważnieni nie muszą włamywać się do systemu, ponieważ są oni częścią systemu. Działania te są dokonywane przez osoby posiadające pewne uprawnienia lub rozszerzające uprawnienia w celu osiągniecia korzyści materialnych lub awansu. Dokonują wielokrotnych ataków w różnych odstępach czasu, narażając się na zdemaskowanie. Rysunek 2 przedstawia strukturę ataków na przedsiębiorstwa.



Rys. 2. Ataki na przedsiębiorstwo
Źródło: opracowanie własne na podstawie danych GUS.

Zagrożenia ze strony nieupoważnionych użytkowników stanowią największą liczbę problemów, jeśli chodzi o następstwa tego typu włamań. Często zagrożenia ze strony użytkowników wewnętrznych są bagatelizowane. Nie jest to poprawne podejście, ponieważ szacunki wskazują, że 60% ataków jest dokonywanych przez użytkowników wewnętrznych. Administratorzy systemów informacyjnych są grupą uprzywilejowaną, jeśli chodzi o uprawnienia. Mają dostęp do wszystkich danych, mogą wszystkie dane odczytywać, zapisywać i modyfikować. Swoje działania bez problemu są w stanie ukryć.

Metody ochrony informacji

Ze względu na występowanie rożnych kategorii zagrożeń związanych z eksploatacją systemów informacyjnych muszą być podejmowane odpowiednie działania zabezpieczające. Ciągłe zmiany w pracujących systemach powodują, że pojedyncze zabezpieczenia nie są w stanie w pełni rozwiązać problemów bezpieczeństwa. Niezbędne jest wprowadzenie różnorodnych metod i narzędzi zabezpieczających. Kompleksowe rozwiązania powinny obejmować zarówno środki techniczne, proceduralne, jak i organizacyjne. Jest to realizowane poprzez opracowanie właściwej dla danej instytucji polityki bezpieczeństwa. Każda instytucja musi zdecydować, które zagrożenia są dla niej istotne i jakie są ich skutki finansowe i moralne. Poprawnie skonstruowana polityka bezpieczeństwa powinna uwzględniać dwie podstawowe metody związane z bezpieczeństwem systemów informatycznych przechowujących dane. Do metod tych należą:

- ograniczenie dostępu,
- zastosowanie metod kryptograficznych,
- dostęp do zasobów poprzez identyfikacje, uwierzytelnianie i autoryzacje.

W badaniach przeprowadzonych w 2008 roku przez stowarzyszenie ITPCG w 235 firmach sprawdzano reakcje na prośby o udostępnienie informacji. Celem testu była pomoc firmom w skutecznym i dokładnym spełnieniu wymagań prawnych, czyli poprawa skuteczności zabezpieczenia informacji na potrzeby postępowania sądowego. Określono ilość informacji podlegających prośbom o udostępnienie. Brano pod uwagę tylko informacje przechowywane w postaci elektronicznej. Informacje przechowywane w postaci elektronicznej stanowiły od 50 do 70% danych w dużych przedsiębiorstwach, od 35 do 50% w firmach średniej wielkości i od 20 do 35% w małych firmach. Większa ilość informacji przechowywanej w postaci elektronicznej zapewnia szybszy dostęp, kompletność oraz poprawność informacji. Z raportu wynika jednak, że te korzyści mają wpływ na obsługę próśb o udostępnienie tylko wtedy, gdy dane są uporządkowane oraz istnieją wbudowane mechanizmy przyspieszające wyszukiwanie, ochronę, przechowywanie i pobieranie danych [1]. Kontrola dostępu do danych jest podstawowym zagadnieniem bezpieczeństwa, nie tylko ze względu na stosowane rozwiązania techniczne, ale również z uwagi na konieczność poprawnego przypisania reguł dostępu do informacji dla poszczególnych użytkowników. Celem kontroli dostępu jest ograniczenie uprawnień użytkownika do minimum wymaganego do pracy w danym systemie informacyjnym. Najczęściej stosowanymi obecnie sposobami realizacji kontroli dostępu są: listy kontroli oraz obowiązkowa i uznaniowa kontrola dostępu.

Najpowszechniejszą metodą kontroli dostępu są tzw. listy kontroli dostępu (ang. Access Control Lists). W praktyce podczas realizacji tworzone są listy

użytkowników, dla każdego elementu bazy danych oraz aplikacji, dla osób, które będą miały do nich dostęp. Jeżeli trzeba dodać lub odebrać dostęp do obiektu, wystarczy zmodyfikować odpowiedni wpis na liście kontroli dostępu. Dodawanie uprawnień jest uwarunkowane stanowiskiem pracy użytkownika i wykonywanymi obowiązkami. Można dopisać użytkownika jedynie do tych obiektów, z których będzie korzystał. Jeżeli użytkownik zmienia stanowisko lub jest zwalniany, należy ręcznie usunąć wszystkie wpisy z list dostępu do obiektów, do których miał dostęp. Takie rozwiązanie niesie za sobą duże prawdopodobieństwo prawidłowego przypisania uprawnień lub usunięcia dostępu.

W obowiązkowej kontroli dostępu (ang. Mandatory Access Control) stosuje się środki ograniczające dostęp do obiektów w oparciu o etykiety bezpieczeństwa i systemowe reguły dostępu. Każdy obiekt danych jest oznaczany pewnym poziomem tajności ze względu na ważność, wrażliwość i wielkość potencjalnych szkód wynikających z ich ujawnienia. Każdy użytkownik otrzymuje dostęp do obiektu, jeśli spełnia wymagania procedury zapewnienia bezpieczeństwa. Tworzona jest hierarchiczna struktura etykiet bezpieczeństwa, które pozwalają przypisać użytkownikom określony poziom bezpieczeństwa dostępu do danych (np. tajne, ściśle tajne, zastrzeżone). Dostęp do określonego obiektu danych mogą mieć tylko użytkownicy z odpowiednimi uprawnieniami. Mechanizm obowiązkowej kontroli można przedstawić za pomocą następujących dwóch podstawowych zasad:

- dostęp do odczytu polega na tym, że przypisany użytkownik ma określony poziom dostępu bezpieczeństwa do odczytu danych, więc nie może przeczytać danych o wyższym poziomie bezpieczeństwa,
- dostęp do zapisu w górę danych na wyższym poziomie bezpieczeństwa powoduje blokadę zapisu danych o niższym poziomie bezpieczeństwa, jeżeli użytkownik ma określony wyższy poziom bezpieczeństwa do zapisu danych [2].

W przypadku kontroli uznaniowej (ang. Discretionary Access Control) dany użytkownik będzie zwykle miał różne uprawnienia do rożnych obiektów. Różni użytkownicy mogą mieć różne prawa dostępu do np. czytania, modyfikowania lub usuwania do tego samego obiektu. Uznaniowe sposoby kontroli są więc bardzo elastyczne. Właściciel obiektu, może kontrolować do niego dostęp i decydować, którzy użytkownicy, jakie prawa dostępu będą do niego posiadali. W momencie, gdy użytkownik nie posiada dostępu do określonego źródła danych, serwer sprawdza uprawnienia użytkownika. Jeżeli przyznane mu uprawnienia są wystarczające, wówczas użytkownik może korzystać z danych, w przeciwnym wypadku dostęp zostaje zabroniony [4].

Na poziomie technicznym kontrola dostępu sprowadza się do:

- identyfikacji,
- uwierzytelniania,

– autoryzacji.

Istotą identyfikacji jest sprawdzanie, kto próbuje uzyskać dostęp do danych i w jaki sposób chce je wykorzystać. Jest to proces umożliwiający rozpoznawanie użytkownika lub obiektu opisanego w systemie informacyjnym. Rozpoznawanie polega na odczytaniu unikatowych cech. Prostym przykładem identyfikacji może być podanie swego imienia. Przykładowo użytkownik A pyta swego partnera o imię i po uzyskaniu odpowiedzi - B bezkrytyczne zakłada jego prawdziwość, prawdopodobieństwo fałszywej akceptacji jest tu stuprocentowo niemożliwe. Może się zdarzyć, że podejrzliwy użytkownik A zakłada stuprocentowe oszustwo rozmówcy, nie dając prawdziwemu użytkownikowi B żadnych szans na konwersację, zabezpiecza się w ten sposób przed podstępem ze strony intruza, odrzucając jednak wszelkie próby nawiązania konwersacji. Jest oczywiste, że w przypadku protokołu identyfikacyjnego obydwie wartości prawdziwa i fałszywa, jako prawdopodobieństwa zdarzeń niepożądanych, powinny być jak najmniejsze [5].

Użytkownik zainteresowany uzyskaniem dostępu do danych chronionych musi udowodnić, że jest tą osobą, za którą się podaje. Może to być realizowane poprzez podanie informacji znanej tylko dla niego lub wykazanie się posiadaniem rzeczy go identyfikującej. Tabela 1 przedstawia metody uwierzytelniania.

Tabela 1. Metody uwierzytelniania

Metoda uwierzytelniania	Przykład
Oparta na wiedzy użytkownika	Hasła Numery identyfikacyjne Słowa kluczowe znane tylko użytkownikowi
Oparta na rzeczach materialnych	Klucze Tokeny Karty szyfrujące Karty identyfikacyjne Certyfikaty i klucze prywatne
Biometryczna	Linie papilarne Kształt twarzy lub dłoni Rysunek tęczówki oka Głos Kod DNA
Oparta na możliwości wykonania	Podpis odręczny Sposób pisania na klawiaturze

Źródło: opracowanie własne na podstawie ISO 27001.

W procesie uwierzytelniania system upewnia się co do tożsamości użytkownika w celu przyznania odpowiednich uprawnień czy przywilejów. Żadna

z powyższych metod nie daje stuprocentowej pewności. W praktyce stosuje się jednocześnie kilka metod, by poprawnie przyznać uprawnienia i tym samym osiągnąć wysoki stopień bezpieczeństwa. Autoryzacja (ang. Authorization), zwana również upoważnianiem, potwierdza, czy dany użytkownik jest uprawniony do korzystania z danych informacji. Upoważnienie może nastąpić jedynie po poprawnej identyfikacji oraz uwierzytelnieniu użytkownika.

Metody kryptograficzne

Kryptografia jest dziedziną nauki zajmującą się zamianą informacji z postaci jawnej na utajnioną, czyli szyfrowaniem. Proces szyfrowania jest odwracalny, pod warunkiem, że znany jest klucz szyfrowania. Znając klucz, można z postaci zaszyfrowanej zawsze otrzymać postać jawną informacji. Proces ten jest zwany odszyfrowywaniem. Algorytmy szyfrowania gwarantują wysokie bezpieczeństwo i jak najmniejszą złożoność obliczeniową procesu szyfrowania i deszyfrowania. Najnowsze techniki tworzenia szyfrów opierają się na wykorzystaniu statystyki matematycznej, jak analiza różnicowa i liniowa. Analizując dany system kryptograficzny, zawsze bierze się pod uwagę metodę szyfrowania i deszyfrowania oraz znane sposoby złamania danego szyfru. Szyfr jest bezwarunkowo bezpieczny, gdy spełnione są warunki:

- długość klucza powinna być taka jak długość tekstu jawnego lub większa,
- klucz musi być ciągiem losowym,
- klucz może być użyty tylko raz [6].

Jeśli są spełnione te warunki, szyfrogram uznawany jest za bezpieczny, gdyż złamanie jego zabezpieczenia jest nieopłacalne. Nakłady czasowe przekraczają okres ochrony informacji lub nakłady pieniężne – wartość odszyfrowywanych danych. Pomiędzy nadawcą i odbiorcą szyfru może nastąpić jego przechwycenie przez osoby nieupoważnione. Osoba przechwytująca może tylko odczytać szyfrogram, nie modyfikując jego treści. W tym przypadku narusza jedynie poufność danych. Jeżeli nieupoważniona osoba po przechwyceniu szyfrogramu dokona modyfikacji, to naruszy autentyczność danych. Aby zachować poufność danych, należy chronić przekształcenie deszyfrujące.

Nieupoważniona osoba ingerująca w wiadomość nie może odczytać danych na podstawie przechwyconego szyfrogramu. Aby zachować autentyczność, należy chronić przekształcenie szyfrujące. Każda próba zastąpienia szyfrogramu oryginalnego szyfrogramem zmienionym powinna być niezwłocznie wykryta. Obecnie w zastosowaniach komercyjnych wykorzystywane są dwa typy algorytmów szyfrujących: symetryczne i asymetryczne. W algorytmach symetrycznych do szyfrowania i odszyfrowywania używa się tego samego klu-

cza. Kryptografia symetryczna jest stosowana do dużych strumieni danych. Zapewnia doskonałą ochronę szyfrowanych danych. Najpopularniejsze szyfry to: DES (ang. Data Encryption Standard) oraz AES (ang. Advanced Encryption Standard). W symetrycznym szyfrowaniu do szyfrowania i deszyfrowania wykorzystuje się ten sam tajny klucz. Przekształcenie szyfrujące oraz deszyfrujące są ze sobą ściśle związane, w związku z tym oba przekształcenia powinny podlegać ochronie, zapewniając tym samym zarówno poufność, jak i autentyczność. Znajomość klucza przez obie strony nie zapewnia niezaprzeczalności autorstwa. Nadawca może zaprzeczyć wysłaniu wiadomości.

W szyfrowaniu asymetrycznym korzysta się z dwóch kluczy. Klucz jawny publiczny i klucz tajny prywatny są komplementarne. Zwykle klucz publiczny służy do szyfrowania, a klucz prywatny do odszyfrowywania, ale nie jest to regułą. Znajomość klucza publicznego nie wpływa na procedurę deszyfrowania, ponieważ nie może być wykorzystany do otrzymania klucza prywatnego. Szyfrowanie z wykorzystaniem klucza publicznego charakteryzuje się umiarkowaną złożonością obliczeniową. Popularne algorytmy asymetryczne to RSA i ELGamal. W systemach kryptograficznych z kluczem publicznym poufność i autentyczność zapewnia się oddzielnymi przekształceniami. System taki może zapewniać poufność lub autentyczność, będąc też zarówno poufnym, jak i autentycznym.

Wnioski

Zapewnienie pełnego bezpieczeństwa danych w praktyce nie jest możliwe. Znane obecnie metody ochrony nie są doskonałe. Nie można przewidzieć wszystkich zagrożeń i ich wyeliminować. Można wskazać newralgiczne dane i miejsca systemu informacyjnego oraz dobrać środki zabezpieczające. Wybierając narzędzia i technologie ochrony danych, należy na początku określić cele, jakim mają służyć. Mechanizmy zabezpieczające muszą być adekwatne do stawianych celów.

Literatura

[1] Babula K.: Skuteczne metody ochrony obniżają koszty, http://pcarena.pl/news/show/84913/Skuteczne-metody-ochrony-obnizaja-koszty.html, 1.02.2013.
[2] Ferraiolo D., Kuhn D., Chandramouli R.: Role-Based Access Control, Artech House, Norwood, 2003.
[3] Kenan K.: Kryptografia w bazach danych. Ostatnia linia obrony, PWN, Warszawa, 2007.

[4] Kozielski S., Małysiak B., Kasprowski P., Mrozek D. (red.): Rozdział. monografii: eBazy danych, struktury, algorytmy, metody,
[5] http://zti.polsl.pl/bdas/2006/BDAS%6006%20%20Kontrola%20dost%C4%99pu%20w%20oparciu%20o%20role.pdf?Id=342&val=1, 1.02.2013.
[6] Pieprzyk J., Hardjono T., Seberry J.: Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice, 2005.
[7] Schneier B.: Kryptografia dla praktyków, WNT, Warszawa, 1995.
[8] Standard ISO 27001.
[9] Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa, 2001.

Ewa Staniewska, Justyna Żywiołek
Politechnika Częstochowska

TOOLS AND TECHNOLOGIES DATA PROTECTION

Abstract

Information as the greatest good of each institution should be protected from unauthorized access, destruction, or unauthorized modification. The paper presents selected aspects of security, in particular the types of threats and methods of data protection.

Keywords: data security, information protection tools.