ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: INFORMATYKA z. 36 Nr kol. 1414

Wojciech FEDYK
T.U. i R. „WARTA" S.A. – Oddział w Bydgoszczy

KRYTYCZNE OBSZARY DLA BEZPIECZEŃSTWA WEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO FIRMY UBEZPIECZENIOWEJ

Streszczenie. W niniejszym artykule przedstawiono próbę wyznaczenia krytycznych obszarów dla bezpieczeństwa wewnętrznego korporacji ubezpieczeniowej. Problem rozważono z uwzględnieniem wielu płaszczyzn funkcjonowania tego typu firmy.

CRITICAL FIELDS FOR SECURITY OF INTERNAL COMPUTER SYSTEM OF AN INSURANCE COMPANY

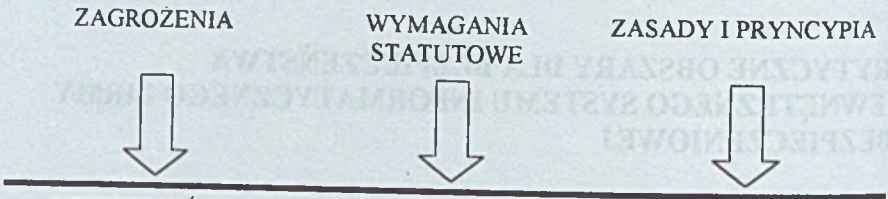
Summary. I this article an attempt to mark critical fields for internal security of insurance corporations have been presented. The problem has been considered with regard to many planes of functioning of such companies.

1. Wprowadzenie

Współczesne firmy, zajmujące się profesjonalnie działalnością finansowo-ubezpieczeniową, wdrażając w swych strukturach nowoczesne systemy komputerowe, stanęły przed nowymi zagrożeniami związanymi z koniecznością zapewnienia ciągłości pracy tych systemów, a przede wszystkim ochroną informacji w nich przetwarzanych. Rodzaj prowadzonej działalności i uzyskiwane wysokie obroty finansowe przyczyniają się do eskalacji potencjalnych zagrożeń. Również coraz silniejsza walka konkurencyjna na polskim rynku ubezpieczeniowym przyczynia się do wzrostu zagrożeń.

Zdefiniujmy trzy główne źródła konieczności zapewnienia bezpieczeństwa systemu informatycznego w korporacji ubezpieczeniowej:

- pewien unikalny dla organizacji zbiór zagrożeń wynikających zarówno z celowych działań, jak również bezbronność systemu w stosunku do posiadanych zbiorów i potencjalnego zagrożenia interesów organizacji,
- zbiór wymagań statutowych i kontraktowych organizacji, partnerów handlowych, kontrahentów i świadczących serwis,
- zbiór głównych pryncypiów i zasad, a także potrzeb w zakresie systemu przekazywania danych, który organizacja stworzyła w celu usprawnienia swego działania.



Rys. 1. Źródła konieczności zapewnienia bezpieczeństwa systemu informatycznego
Fig. 1. Sources of necessity to guarantee security of computer system

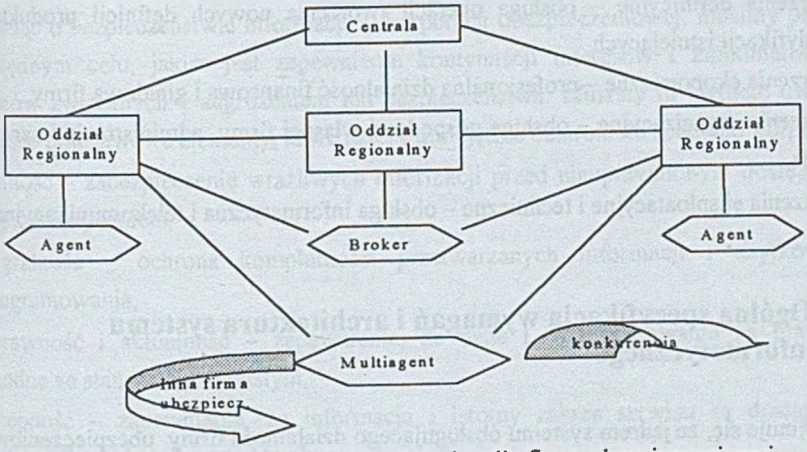
2. Specyfika organizacji

Każda korporacja ubezpieczeniowa charakteryzuje się wielostopniową strukturą organizacyjną. Ma to bezpośredni wpływ na zadania realizowane przez poszczególne jednostki organizacyjne. Wyróżniamy Centralę, Oddziały Regionalne, w skład których mogą wchodzić Inspektoraty, Przedstawicielstwa, Filie, w zależności od specyfiki ubezpieczeniowej. Na najniższym szczeblu struktury znajdują się agenci i multiagenci ubezpieczeniowi oraz brokerzy.

Każda z jednostek organizacyjnych w zależności od położenia w strukturze firmy posiada własny zakres kompetencji i wykonywanych funkcji. Funkcje te rzutują w sposób zdecydowany na możliwość wyodrębnienia istotnych zadań realizowanych przez poszczególne jednostki. Zadania te będą miały kluczowe znaczenie w sensie zapewnienia im szczególnej ochrony w zintegrowanym systemie informatycznym korporacji. I tak, im jednostka znajduje się wyżej w hierarchii organizacji, tym jej zadania koncentrują się bardziej na:

- określaniu wstępnych warunków ubezpieczeń,
- wprowadzaniu nowych produktów,
- przeprowadzaniu badań i analiz (portfel ubezpieczeń, taryfy, szkodowość, pole ubezpieczeniowe, itp.),
- przeprowadzaniu analiz,

- obsłudze reasekuracji i działalności lokacyjnej,
- promocji i działalności marketingowej.



Rys. 2. Przykładowa struktura organizacyjna dla firmy ubezpieczeniowej
Fig. 2. An example of organizational structure for insurance company

Obiekty organizacyjne umiejscowione na niższym szczeblu struktury realizują zadania związane z podstawową działalnością operacyjną, a więc:

- przeprowadzanie szczegółowych analiz i badań szkodowości (klientów, pośredników, agentów, brokerów i multiagentów),
- działalność operacyjna (poważniejsze umowy i ubezpieczenia),
- integracja danych statystycznych i wyników finansowych w ramach regionu,
- gromadzenie danych o klientach i kontrahentach firmy,
- sprzedaż produktów ubezpieczeniowych i likwidacja szkód,
- przygotowywanie danych statystycznych i finansowych z działalności operacyjnej,
- rozliczanie pośredników i agentów ubezpieczeniowych pod względem poprawności merytorycznej zawartych umów, finansowym i druków ścisłego zarachowania,
- kontrola płatności klientów,

Część jednostek dzieli się dodatkowo na działy, referaty i stanowiska merytorycznie odpowiedzialne za realizację różnych zadań. W sumie daje to dość złożoną strukturę w sensie wypracowania polityki bezpieczeństwa.

Z tak zdefiniowanej, ogólnie pojętej działalności poszczególnych komponentów organizacji firmy wynikają wspólne dla wszystkich szczebli zjawiska, które nazwiemy zdarzeniami ubezpieczeniowymi. Określenie zdarzeń ubezpieczeniowych ma duże znaczenie dla dalszych rozważań nad bezpieczeństwem systemu informatycznego w korporacji.

Ze względu na swój charakter zdarzenia dzielą się na:

- zdarzenia operacyjne – inicjacja działalności operacyjnej na różnych szczeblach,

- zdarzenia sprawozdawczo-analityczne – inicjalizacja działalności sprawozdawczej na wszystkich szczeblach działalności,
- zdarzenia definicyjne – obsługa operacji tworzenia nowych definicji produktów lub modyfikacji istniejących,
- zdarzenia ekonomiczne – profesjonalna działalność finansowa i giełdowa firmy,
- zdarzenia organizacyjne – obsługa gospodarki własnej firmy, administracja i zarządzanie firmą,
- zdarzenia eksploatacyjne i techniczne – obsługa informatyczna i telekomunikacyjna,

3. Ogólna specyfikacja wymagań i architektura systemu informatycznego

Przyjmuje się, że jądrem systemu obsługującego działalność firmy ubezpieczeniowej jest szereg relacyjnych baz danych, osadzonych w środowisku sieciowego lub wielodostępnego systemu operacyjnego (np. UNIX) z możliwością zdalnego dostępu do nich z innych sieci lokalnych (np. Novell NetWare, Windows NT) oraz stacji roboczych (pracujących w środowisku DOS/Windows). Aplikacje są przystosowane do pracy w rozległym środowisku sieciowym, np. opartym na standardzie Frame Relay. W związku z tym konstrukcja baz danych musi zapewniać możliwie dużą niezależność od oprogramowania, szczególnie w zakresie kontroli logicznej spójności danych. Dla potrzeb zarządzania bazą danych zostaną użyte narzędzia 4GL (Sybase, Oracle, Progress lub Informix Online).

System informatyczny musi być skonstruowany tak, że będzie zapewniał wymóg zintegrowanego oprogramowania zawierającego następujące obszary zagadnieniowe:

- produkty ubezpieczeniowe,
- klienci i kontrahenci firmy,
- druki ścisłego zarachowania,
- umowy agencyjne,
- polisy,
- umowy reasekuracyjne,
- statystykę ubezpieczeniową,
- analizy aktuarialne i marketingowe,
- F-K, kadry – płace, zlecenia,
- likwidacja szkód,
- elektroniczna wymiana informacji, dokumentów i pieniędzy z bankami i innymi kontrahentami,
- inne.

4. Obszary krytyczne dla bezpieczeństwa systemu

Mówiąc o bezpieczeństwie informacji w korporacji ubezpieczeniowej, musimy pamiętać o nadrzędnym celu, jakim jest zapewnienie kontynuacji interesów i zminimalizowanie incydentów związanych z zagrożeniem ich bezpieczeństwa. Musimy tu zwrócić uwagę na następujące podstawowe elementy, które należy umiejętnie dostroić do specyfiki korporacji:

- poufność – zabezpieczenie wrażliwych informacji przed nieuprawnionym dostępem lub ich przechwyceniem,
- integralność – ochrona kompletności przetwarzanych informacji i użytkowanego oprogramowania,
- poprawność i aktualność – zapewnienie, że dane i oprogramowanie są prawdziwe i zgodne ze stanem rzeczywistym,
- dostępność – zapewnienie, że informacja i istotny zakres serwisu są dostępne dla użytkownika, gdy tylko są potrzebne.

Innym bardzo ważnym etapem w procesie projektowania systemu bezpieczeństwa jest wskazanie i rozróżnienie wszystkich udziałowców systemu oraz określenie zakresu ich kompetencji i obowiązków. Bezpośrednimi udziałowcami systemu są:

- administratorzy sieci rozległej,
- administratorzy systemów operacyjnych,
- administratorzy relacyjnych baz danych,
- administratorzy poczty elektronicznej,
- administratorzy aplikacji,
- administrator sytemu zarządzania systemem,
- użytkownicy aplikacji,
- projektanci mechanizmu zarządzania systemem.

Ze względu na wszystkie wymienione wyżej uwarunkowania związane ze specyfiką funkcjonowania istnieje konieczność wyznaczenia krytycznych obszarów mających wpływ na bezpieczeństwo systemu informatycznego firmy. Jest to czynnik niezbędny do wypracowania przyszłej polityki bezpieczeństwa w firmie o takim profilu działalności. Wydawać by się mogło, że jest to zadanie w pełni do powielenia dla wszystkich instytucji, bez względu na profil prowadzonej działalności. Takie podejście nie jest jednak prawdziwe w przypadku firmy ubezpieczeniowej, która jest narażona na pewne specyficzne formy zagrożeń i działalności przestępczej w ramach funkcjonującego systemu komputerowego. Na przykład, dla firmy ubezpieczeniowej okresowa utrata dostępności do danych systemu komputerowego nie jest czynnikiem krytycznym i determinującym, jak to ma miejsce w przypadku systemów bankowych lub systemów sprzedaży. Dopuszcza się tu nawet

możliwość bezruchu trwającego kilka dni (max. do 7). Natomiast utrata danych, utrata poufności nawet w niewielkim zakresie powoduje w konsekwencji ogromne straty.

Dodatkowym elementem wyróżniającym firmy ubezpieczeniowe pod względem potencjalnych zagrożeń jest fakt rejestrowania corocznie przez te firmy ogromnych strat spowodowanych pewną kategorią przestępstw, jakie zostały zdefiniowane w prawie jako przestępstwa ubezpieczeniowe. Wraz z wkroczeniem w progi instytucji ubezpieczeniowych systemów komputerowych ujawniły się również nowe formy szeroko rozumianych zagrożeń dla interesów firmy. Dodatkowym utrudnieniem i potencjalnym zagrożeniem jest fakt, że wszystkie projekty informatyczne dla tego typu firm są ogromnymi przedsięwzięciami, zawsze o zasięgu ogólnokrajowym.

Możliwe do zdefiniowania zagrożenia dla systemu informatycznego firmy zajmującej się działalnością finansowo-ubezpieczeniową mają ścisłe odzwierciedlenie we wszystkich płaszczyznach systemu informatycznego. Możemy zdefiniować następujące płaszczyzny, w które wkomponowany jest system komputerowy:

- organizacja firmy,
- specyfika działalności ubezpieczeniowej,
- zarządzanie,
- stosowana technologia i infrastruktura informatyczna,
- aktualnie obowiązujące prawo,
- współpraca firmy z otoczeniem.

Dopiero wyznaczenie wymienionych wyżej płaszczyzn, z którymi ściśle wiążą się zagrożenia, pozwala poprzez dalsze uszczegółowienie wyznaczyć właściwe obszary krytyczne dla bezpieczeństwa systemu informatycznego.

4.1. Płaszczyzna organizacyjna firmy

Znajdujemy w niej następujące krytyczne obszary stanowiące potencjalne, poważne zagrożenie dla bezpieczeństwa firmy:

- hierarchiczna budowa systemu,
- przestrzenne rozmieszczenie elementów systemu,
- podział na działy i stanowiska merytoryczne.

4.2. Płaszczyzna działalności ubezpieczeniowej

Znajdujemy następujące krytyczne obszary stanowiące potencjalne, poważne zagrożenie dla bezpieczeństwa firmy:

- taktyka i działalność inwestycyjna firmy,
- własne dane finansowe i statystyczne,

- dane o klientach,
- likwidacja szkód,
- strategie ubezpieczeń,
- zawieranie i obsługa umów ubezpieczenia,
- obsługa płatności składek,
- rozliczanie pośredników i agentów.

4.3. Płaszczyzna zarządzania

Znajdujemy następujące krytyczne obszary stanowiące potencjalne, poważne zagrożenie dla bezpieczeństwa firmy:

- polityka kadrowo-płacowa;
- kryteria odpowiedzialności – wiążą się ściśle z precyzyjnym podziałem zadań i kompetencji za sprawne funkcjonowanie systemu informatycznego na wszystkich jego szczeblach. Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to konieczność wyznaczania:
  a) osób odpowiedzialnych za nadzór nad bezpieczeństwem systemu,
  b) osób odpowiedzialnych za kontrolę i analizę systemu zabezpieczeń,
  c) osób odpowiedzialnych za fizyczną ochronę składników systemu informatycznego,
  d) osób odpowiedzialnych za archiwizację i wykonywanie kopii bezpieczeństwa danych,
  e) osób odpowiedzialnych za szkolenie w tym zakresie,
  f) osób odpowiedzialnych za kontrolę poprawności danych wprowadzanych w systemie;
- organizacja pracy z wykorzystaniem systemu informatycznego:
  a) wyznaczenie terminów dostępu do danych dla poszczególnych stanowisk i działów,
  b) wyznaczenie określonych zakresów funkcjonalnych możliwych do wykonania w systemie przez poszczególnych pracowników i działy,
  c) wyznaczenie stałych terminów czynności konserwacyjnych i serwisowych fizycznych elementów systemu,
  d) wyznaczenie stałych terminów czynności technologicznych związanych z serwisem oprogramowania,
  e) wyznaczenie stałych terminów wykonywania zabezpieczeń i backup.

4.4. Płaszczyzna stosowanej technologii i infrastruktury informatycznej

Znajdujemy następujące krytyczne obszary stanowiące potencjalne, poważne zagrożenie dla bezpieczeństwa firmy:

- Systemy operacyjne będą stanowiły podstawową platformę działania i współdziałania systemów. Elementy krytyczne dla systemu operacyjnego to:

a) kluczowe dla systemu operacyjnego (syslogd,cron,errorlogd),
b) związane ze zdalnym dostępem (inetd,nfsd,biod),
c) związane z zarządzaniem (snmpd).

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to konieczność zapewnienia kontroli polegającej na stałym sprawdzaniu, czy:

a) nie podejmowano kilkukrotnej, nieudanej próby wejścia na konto użytkownika root,
b) były próby wejścia do systemu określoną ilość razy,
c) istnieją w systemie użytkownicy bez hasła,
d) istnieją w systemie użytkownicy z uprawnieniami administracyjnymi systemu,
e) dokonano zmian w systemowych plikach bezpieczeństwa i logach systemowych,
f) dokonano zmian ilości i stanu plików SUID i SGID przynależnych do użytkowników administrujących systemem, bazami danych i aplikacją.

- Bazy danych i narzędzia do ich przetwarzania. Elementy bezpieczeństwa, przy uwzględnieniu środowiska np. INFORMIX ONLINE, które można wyróżnić w tym obszarze, to konieczność zapewnienia:
  a) zabezpieczenia narzędzi SQL przed nieautoryzowanym dostępem,
  b) składowania logów logicznych,
  c) sprawdzania procentowej zajętości dziennika transakcji (logical logs),
  d) monitorowania obecności procesu odpowiedzialnego za kopiowanie dziennika,
  e) monitorowania liczby logów złożonych na taśmie od ostatniej archiwizacji,
  f) archiwizacji obszarów bazy danych (1 – 2) razy dziennie; backup pełny i przyrostowy,
  g) monitorowania obecności procesów systemowych związanych z motorem bazy danych (tbinit,tbpgcl),
  h) monitorowania statusu motoru bazy danych (off-line, recovery, quiescent, on-line, shutdown),
  i) sprawdzania stanu zajętości obszarów dbspace i blobspace,
  j) sprawdzania stanu porcji dyskowych (chunks), wykrywanie wyłączonych,
  k) wykonywania update statistic,
  l) przeglądania dziennika komunikatów.
- Oprogramowanie aplikacyjne
  Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to:
  a) nadanie uprawnień użytkownikom do funkcji aplikacji,
  b) okresowe sprawdzanie konfiguracji aplikacji,
  c) ochrona zmiennych systemowych aplikacji,
  d) ochrona drivera głównego aplikacji,
  e) sprawdzanie fizycznej spójności danych,

f) sprawdzanie transakcyjności baz danych,
g) sprawdzanie trybu lokowania tablic.

- Serwery

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to:

a) ochrona fizyczna serwera,
b) reakcja na zaniki napięcia,
c) kontrola wykorzystania pamięci wirtualnej (swap space),
d) kontrola wykorzystania procesora,
e) kontrola urządzeń dyskowych,
f) kontrola napędów taśm magnetycznych.

- Stacje robocze i urządzenia peryferyjne

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to:

a) ochrona hasłem na poziomie BIOSu wszystkich komputerów personalnych,
b) aktywna ochrona antywirusowa,
c) aktywna kontrola wykorzystania stacji roboczej (pliki raportów),
d) monitorowanie stacji roboczych pracujących w sieci: nazwa, typ sprzętu, wersja systemu operacyjnego, lokalizacja (z bazy MIB),
e) monitorowanie interfejsów stacji (ich adresy i stan).

- Elementy aktywne i pasywne sieci

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to:

a) ograniczenie dostępu do szafy dystrybucyjnej okablowania strukturalnego,
b) ochrona routerów,
c) ochrona koncentratorów,
d) fizyczne odłączenie nie używanych gniazd,
e) monitorowanie obciążenia sieci.

- Transmisja danych w sieci rozległej

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze to:

a) szyfrowanie danych,
b) ustalenie tożsamości nadawcy i odbiorcy,
c) niezaprzeczalność nadania,
d) podpis cyfrowy.

- Postępowanie z nośnikami magnetycznymi i wydrukami

Elementy bezpieczeństwa, które można wyróżnić w tym obszarze, to:

a) ścisła rejestracja wydruków i nośników magnetycznych,
b) ochrona drukarek przed nieautoryzowanym dostępem,
c) kontrola dostępu do kolejek drukarkowych, stacji dysków i steamerów,

d) niszczenie bezużytecznych wydruków i nośników magnetycznych,
e) bezpieczne przechowywanie wydruków i nośników magnetycznych.

4.5. Płaszczyzna aktualnie obowiązującego prawa

Znajdujemy następujące krytyczne obszary stanowiące potencjalne, poważne zagrożenie dla bezpieczeństwa firmy:

- ochrona programów komputerowych – zgodna z Ustawą „o prawie autorskim i prawach pokrewnych" z dnia 4 lutego 1994 r.
- ochrona danych osobowych zgodna z Ustawą „o ochronie danych osobowych" z dnia 29 sierpnia 1997 r.
- sposób przetwarzania i ochrona danych finansowych – zgodna z Ustawą „o rachunkowości" z dnia 29 września 1994 r.
- ochrona przed nieuczciwą konkurencją,
- ochrona przed pospolitymi przestępstwami z użyciem nowoczesnych technik komputerowych – w odniesieniu do Kodeksu Karnego (oszustwo, kradzież, sabotaż, fałszerstwo, włamanie, wyłudzenie, podsłuch, uszkodzenie).

4.6. Płaszczyzna ścisłej współpracy firmy z otoczeniem

- Internet
- transakcje bezgotówkowe z bankami i innymi instytucjami
- dane zasilające z zewnątrz

5. Podsumowanie

Podsumowując, należy stwierdzić, iż zadanie stworzenia kompleksowej ochrony interesów biznesowych firmy ubezpieczeniowej poprzez zapewnienie pełnego bezpieczeństwa stosowanego w niej systemu informatycznego jest przedsięwzięciem złożonym i w pewnym sensie nowatorskim w warunkach polskich.

Najistotniejsze zadania wymagające natychmiastowej realizacji w najbliższej przyszłości to:

- Opracowanie strategicznych dokumentów związanych z projektem, wdrożeniem i stosowaniem zaleceń odnośnie do stosowanych procedur bezpieczeństwa i zintegrowanego zarządzania systemem,
- pełna integracja heterogenicznych sieci komputerowych,

- zapewnienie poufności i integralności przesyłanych informacji oraz kontroli dostępu do zasobów sieci,
- zapewnienie niezawodności, automatycznej rekonfiguracji i alarmowania o sytuacjach awaryjnych,
- zapewnienie dostępu do sieci wszystkim użytkownikom poprzez odpowiednią konfigurację,
- zapewnienie efektywnego zarządzania.

LITERATURA

1. Praca zbiorowa: Systemy komputerowe. PRONET, Gliwice 1994.
2. Grzywak A.: Bezpieczeństwo w systemach rozproszonych. ZN Pol. Śl. s. Informatyka z. 24, Gliwice 1993.
3. Kierzkowski A.: Ochrona programów i danych w praktyce, Helion, Gliwice 1992.
4. Garfinkel S., Spafford G.: Bezpieczeństwo w Unixie i Internecie. Wydawnictwo RM Sp.z o.o., Warszawa 1997.
5. Ustawa „o prawie autorskim i prawach pokrewnych" (Dz. U. z dnia 23 lutego 1994 r.) z dnia 4 lutego 1994 r.
6. Ustawa „o ochronie danych osobowych" (Dz. U. z dnia 29 października 1997 r.) z dnia 29 sierpnia 1997 r.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 1 kwietnia 1999 r.

Abstract

Summarising this article, it should be stated that the task of creating a complex protection of insurance company is business by achieving full security of its computer system is a complicated enterprise, which also proves to be in a way innovative in Polish conditions.

The most important tasks requiring immediate realisation in near future are:

- elaborating strategic documents connected with project, implementation and use of recommendations concerning security procedures and integrated managing system in use,
- full integration of heterogeneous computer networks,

- providing confidentiality and integrity of information sent and controlling the access to the network's resources,
- creating reliability, automatic reconfiguration and alarming in case of emergency,
- creating access to the network to an users through suitable configuration,
- creating effective managing.