DECYZJA KOMISJI

z dnia 16 marca 2007 r.

ustanawiająca wymogi sieciowe dla Systemu Informacyjnego Schengen II (3. filar)

(2007/171/WE)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat o Unii Europejskiej,

uwzględniając decyzję Rady 2001/886/WSiSW z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II) [1], w szczególności jej art. 4 lit. a),

a także mając na uwadze, co następuje:

(1) Aby opracować SIS II, należy określić specyfikacje techniczne dotyczące sieci informatycznej i jej części składowych oraz konkretne wymogi sieciowe.

(2) Powinno się wprowadzić odpowiednie ustalenia, dotyczące w szczególności cech jednorodnego interfejsu krajowego zlokalizowanego w państwach członkowskich, które obowiązywałyby Komisję i państwa członkowskie.

(3) Niniejsza decyzja pozostaje bez uszczerbku dla przyjęcia w przyszłości innych decyzji Komisji odnoszących się do stworzenia SIS II, w szczególności zaś dotyczących dopracowania wymogów bezpieczeństwa.

(4) Rozwój SIS II regulują zarówno przepisy rozporządzenia Rady (WE) nr 2424/2001 [2], jak i decyzji 2001/886/WSiSW. Aby zagwarantować, że tworzenie całego SIS II będzie przebiegać w ramach jednego procesu wdrażania, przepisy niniejszej decyzji powinny stanowić odbicie przepisów decyzji Komisji ustanawiającej wymogi sieciowe dla SIS II, która ma zostać przyjęta na podstawie rozporządzenia (WE) nr 2424/2001.

(5) Niniejsza decyzja ma zastosowanie do Zjednoczonego Królestwa zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy prawne Unii Europejskiej, załączonego do Traktatu UE i Traktatu WE, oraz art. 8 ust. 2 decyzji Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącej wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec niego niektórych przepisów dorobku Schengen [3].

(6) Niniejsza decyzja ma zastosowanie do Irlandii zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy prawne Unii Europejskiej, załączonego do Traktatu UE i Traktatu WE, oraz art. 5 ust. 1 i art. 6 ust. 2 decyzji Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącej wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen [4].

(7) W odniesieniu do Islandii i Norwegii niniejsza decyzja stanowi rozwinięcie dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, które wchodzą w zakres obszaru określonego w art. 1 lit. G decyzji Rady 1999/437/WE [5] w sprawie niektórych warunków stosowania tej umowy.

(8) W odniesieniu do Szwajcarii niniejsza decyzja stanowi rozszerzenie przepisów dorobku Schengen w rozumieniu Umowy podpisanej przez Unię Europejską, Wspólnotę Europejską i Konfederację Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, które mieszczą się w obszarze określonym w art. 1 lit. G decyzji Rady 1999/437/WE rozumianym w powiązaniu z art. 4 ust. 1 decyzji Rady 2004/849/WE [6] w sprawie podpisania w imieniu Unii Europejskiej oraz tymczasowego stosowania niektórych przepisów tej umowy.

(9) Niniejsza decyzja stanowi akt oparty na dorobku Schengen lub jest z nim w inny sposób powiązana w rozumieniu art. 3 ust. 1 Aktu Przystąpienia.

(10) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu powołanego na mocy art. 5 ust. 1 decyzji 2001/886/WSiSW,

---

[1] Dz.U. L 328 z 13.12.2001, str. 1.
[2] Dz.U. L 328 z 13.12.2001, str. 4. Rozporządzenie zmienione rozporządzeniem (WE) nr 1988/2006 (Dz.U. L 411 z 30.12.2006, str. 1).
[3] Dz.U. L 131 z 1.6.2000, str. 43. Decyzja zmieniona decyzją 2004/926/WE (Dz.U. L 395 z 31.12.2004, str. 70).
[4] Dz.U. L 64 z 7.3.2002, str. 20.
[5] Dz.U. L 176 z 10.7.1999, str. 31.
[6] Dz.U. L 368 z 15.12.2004, str. 26.

STANOWI, CO NASTĘPUJE:

Artykuł 1

W załączniku określa się specyfikacje techniczne odnoszące się do projektu fizycznej architektury infrastruktury komunikacyjnej SIS II.

Sporządzono w Brukseli, dnia 16 marca 2007 r.

W imieniu Komisji
Franco FRATTINI
Wiceprzewodniczący

ZAŁĄCZNIK

SPIS TREŚCI

1. **Wprowadzenie**

W niniejszym dokumencie opisano projekt sieci informatycznej i jej części składowych oraz konkretne wymogi sieciowe.

1.1. *Akronimy i skróty*

W niniejszej części przedstawiono akronimy, których użyto w dokumencie.

Akronimy i skróty	Objaśnienie
BLNI	Rezerwowy lokalny interfejs krajowy
CEP	Główny punkt końcowy
CNI	Główny interfejs krajowy
CS	System główny (ang. *Central System*)
CS-SIS	Baza techniczna zawierająca bazę danych SIS II
DNS	Serwer nazw domen (ang. *Domain Name Server*)
FCIP	Technologia *Fibre Channel over IP*
FTP	Protokół przesyłania plików (ang. *File Transport Protocol*)
HTTP	Protokół przesyłania hipertekstu (ang. *Hyper Text Transfer Protocol*)
IP	Protokół IP (ang. *Internet Protocol*)
LAN	Lokalna sieć komputerowa (ang. *Local Area Network*)
LNI	Lokalny interfejs krajowy
Mb/s	Megabity na sekundę
MDC	Główny programista-wykonawca
N.SIS II	Moduł krajowy w każdym państwie członkowskim
NI-SIS	Jednorodny interfejs krajowy
NTP	Protokół synchronizacji czasu (ang. *Network Time Protocol*)
SAN	Sieć pamięci masowej (ang. *Storage Area Network*)
SDH	Synchroniczna hierarchia cyfrowa (ang. *Synchronous Digital Hierarchy*)
SIS II	System Informacyjny Schengen drugiej generacji
SMTP	Protokół SMTP (ang. *Simple Mail Transport Protocol*)
SNMP	Protokół SNMP (ang. *Simple Network Management Protocol*)
s-TESTA	Bezpieczne ogólnoeuropejskie usługi telematyczne między administracjami, stanowiące środek przewidziany w ramach programu IDABC (interoperatywne świadczenie ogólnoeuropejskich usług eGovernment dla administracji publicznej, przedsiębiorstw i obywateli. Decyzja Parlamentu Europejskiego i Rady 2004/387/WE z 21.4.2004).
TCP	Protokół kontroli transmisji (ang. *Transmission Control Protocol*)
VIS	Wizowy system informacyjny
VPN	Wirtualna sieć prywatna (ang. *Virtual Private Network*)
WAN	Rozległa sieć komputerowa (ang. *Wide Area Network*)

2. **Informacje ogólne**

W skład SIS II wchodzą:

— system główny (zwany dalej „głównym SIS II") złożony z:

• bazy technicznej (zwanej dalej „CS-SIS"), zawierającej bazę danych SIS II. Główny CS-SIS odpowiada za nadzór techniczny i administrację, natomiast rezerwowy CS-SIS jest w stanie przejąć wszystkie funkcje głównego CS-SIS w przypadku jego awarii,

• jednorodnego interfejsu krajowego (zwanego dalej „NI-SIS"),

— moduł krajowy (zwany dalej „N.SIS II") znajdujący się w każdym państwie członkowskim, złożony z krajowych systemów danych, które łączą się z głównym SIS II. N.SIS II może zawierać plik danych (zwany dalej „kopią krajową"), w którym znajduje się pełna lub częściowa kopia bazy danych SIS II,

— infrastruktura komunikacyjna pomiędzy CS-SIS a NI-SIS (zwana dalej „infrastrukturą komunikacyjną"), zapewniająca zaszyfrowaną sieć wirtualną przeznaczoną dla danych SIS II oraz umożliwiająca wymianę danych między biurami SIRENE.

NI-SIS składa się z:

— jednego lokalnego interfejsu krajowego (zwanego dalej „LNI") na każde państwo członkowskie; interfejs ten łączy fizycznie państwo członkowskie z bezpieczną siecią i zawiera urządzenia szyfrujące na użytek SIS II i połączeń między biurami SIRENE. LNI jest umieszczony w obiektach zlokalizowanych na terenie państw członkowskich,

— ewentualnie także z rezerwowego lokalnego interfejsu krajowego (zwanego dalej „BLNI"), który składa się z takich samych elementów i pełni taką samą funkcję co LNI.

LNI i BLNI są przeznaczone wyłącznie na użytek systemu SIS II i do wymiany danych między biurami SIRENE. Konkretna konfiguracja LNI i BLNI zostanie określona i uzgodniona z każdym państwem członkowskim osobno, aby uwzględnić wymogi bezpieczeństwa, fizyczne umiejscowienie i warunki instalacji, w tym świadczenie usług przez dostawcę sieci, co oznacza, że fizyczne połączenie s-TESTA może zawierać wiele tuneli VPN na użytek innych systemów, na przykład VIS i Eurodac,

— głównego interfejsu krajowego (zwanego dalej „CNI"), czyli programu zabezpieczającego dostęp do CS-SIS. Każde państwo członkowskie ma osobne punkty dostępu logicznego do CNI poprzez główną zaporę sieciową (ang. *firewall*).

Infrastruktura komunikacyjna pomiędzy CS-SIS a NI-SIS składa się z:

— sieci na potrzeby bezpiecznych ogólnoeuropejskich usług telematycznych między administracjami (zwanej dalej s-TESTA), zapewniającej zaszyfrowaną prywatną sieć wirtualną przeznaczoną dla danych SIS II oraz umożliwiającą wymianę danych między biurami SIRENE.

3. **Zakres terytorialny**

Infrastruktura komunikacyjna musi umożliwić świadczenie koniecznych usług na rzecz wszystkich państw członkowskich.

Dotyczy to wszystkich państw członkowskich UE (Belgia, Francja, Niemcy, Luksemburg, Niderlandy, Włochy, Portugalia, Hiszpania, Grecja, Austria, Dania, Finlandia, Szwecja, Cypr, Republika Czeska, Estonia, Węgry, Łotwa, Litwa, Malta, Polska, Słowacja, Słowenia, Zjednoczone Królestwo i Irlandia), jak również Norwegii, Islandii i Szwajcarii.

Ponadto zasięg tych usług należy rozszerzyć o kraje przystępujące do UE – Rumunię i Bułgarię.

Należy również przewidzieć możliwość rozbudowy infrastruktury komunikacyjnej, tak by objęła swym zasięgiem inne kraje lub podmioty przystępujące do głównego SIS II (np. Europol, Eurojust).

4. **Usługi sieciowe**

Za każdym razem, gdy mowa o danym protokole lub architekturze, należy założyć, że do przyjęcia są również równorzędne im przyszłe technologie, protokoły i architektury.

4.1. *Układ sieci*

Architektura SIS II korzysta ze scentralizowanych usług, do których można uzyskać dostęp z różnych państw członkowskich. Aby zwiększyć niezawodność systemu, te scentralizowane usługi są kopiowane do dwóch różnych miejsc – Strasburga we Francji oraz St Johann im Pongau w Austrii, czyli odpowiednio jednostki głównej (CU) oraz jednostki rezerwowej (BCU) bazy CS-SIS.

Dostęp do jednostek centralnych – głównej i rezerwowej – musi być możliwy z różnych państw członkowskich. Kraje uczestniczące mogą mieć liczne punkty dostępu do sieci oraz posiadać LNI i BLNI, aby łączyć swoje systemy krajowe z usługami centralnymi.

Oprócz swojej podstawowej funkcji, czyli zapewnienia dostępu do usług centralnych, infrastruktura komunikacyjna musi także umożliwiać dwustronną wymianę informacji dodatkowych między biurami SIRENE różnych państw członkowskich.

4.2. *Rodzaj połączenia między głównym CS-SIS a rezerwowym CS-SIS*

Wymagany rodzaj połączenia między głównym CS-SIS a rezerwowym CS-SIS to pierścień SDH lub jego odpowiednik, co oznacza, że musi on być otwarty także na nowe, przyszłe architektury i technologie. Infrastruktura SDH zostanie wykorzystana do tego, by rozszerzyć sieci lokalne obu jednostek centralnych w celu stworzenia ciągłej, pojedynczej sieci LAN. Powstała w ten sposób sieć LAN zostanie następnie wykorzystana do zapewnienia ciągłej synchronizacji między CU i BCU.

4.3. *Szerokość pasma*

Wymogiem o zasadniczym znaczeniu dla infrastruktury komunikacyjnej jest część szerokości pasma, jaką można przyznać różnym połączonym ze sobą miejscom, oraz zdolność utrzymania tej szerokości pasma w sieci szkieletowej.

Szerokość pasma konieczna dla LNI i opcjonalnego BLNI będzie inna dla każdego państwa członkowskiego, głównie w zależności od tego, jakich wyborów dokonano w zakresie korzystania z kopii krajowych, centralnego wyszukiwania i wymiany danych biometrycznych.

To, jaka dokładnie część szerokości zostanie przyznana w ramach infrastruktury komunikacyjnej, nie ma znaczenia, o ile zaspokojone zostaną minimalne potrzeby każdego państwa członkowskiego.

Z każdego z wyżej wspomnianych rodzajów miejsc można przesyłać duże ilości danych (alfanumerycznych, biometrycznych i całych dokumentów) w jedną lub w drugą stronę. W związku z tym infrastruktura komunikacyjna musi zapewniać wystarczającą minimalną gwarantowaną prędkość wysyłania i pobierania danych dla każdego połączenia.

Infrastruktura komunikacyjna musi zapewniać szybkość połączenia w przedziale od 2 Mb/s do 155 Mb/s lub wyższą. Sieć musi zapewniać wystarczającą minimalną gwarantowaną prędkość wysyłania i pobierania danych dla każdego połączenia, a jej przepustowość musi zostać tak dobrana, aby możliwe było obsłużenie całkowitej szerokości pasma punktów dostępu do sieci.

4.4. *Kategorie usług*

Główny SIS II będzie zapewniał możliwość ustalenia priorytetów dla zapytań i wpisów. Osobnym wymogiem stawianym infrastrukturze komunikacyjnej będzie ustalenie priorytetu dla ruchu sieciowego.

Przyjmuje się, że sieciowe priorytety transmisji określa główny SIS II w stosunku do wszystkich pakietów, które tego wymagają. Zostanie do tego wykorzystany ważony sprawiedliwy algorytm kolejkowania (ang. *Weighted Fair Queuing*). Oznacza to, że infrastruktura komunikacyjna musi być w stanie rozpoznać priorytety przypisane pakietom danych w źródłowej sieci LAN oraz zapewnić odpowiednią obsługę tych pakietów w swojej własnej sieci szkieletowej. Ponadto w zdalnie dostępnym miejscu infrastruktura komunikacyjna musi przesłać wysłane pakiety z priorytetem, jaki został ustawiony w źródłowej sieci LAN.

4.5. *Obsługiwane protokoły*

Główny SIS II będzie korzystał z wielu protokołów transmisji sieciowej. Infrastruktura komunikacyjna powinna zapewniać współpracę z szeroką gamą protokołów transmisji sieciowej. Standardowe protokoły, które powinny być obsługiwane, to HTTP, FTP, NTP, SMTP, SNMP i DNS.

Poza standardowymi protokołami infrastruktura komunikacyjna musi także być w stanie obsługiwać różne protokoły tunelowania, protokoły replikacji SAN oraz zastrzeżone protokoły połączeń *Java-to-Java* typu *BEA WebLogic*. Protokoły tunelowania, np. IPsec w trybie tunelowym, zostaną wykorzystane do przesyłania zaszyfrowanych danych do miejsca przeznaczenia.

4.6. *Specyfikacje techniczne*

4.6.1. Adresowanie IP

Infrastruktura komunikacyjna musi mieć szereg zastrzeżonych adresów IP, z których można korzystać wyłącznie w obrębie tej sieci. Główny SIS II będzie korzystał z wydzielonego zakresu adresów IP, wyodrębnionych spośród wyżej wspomnianego zbioru zastrzeżonych adresów IP, który to zakres nie będzie wykorzystywany nigdzie indziej.

4.6.2. Obsługa IPv6

Można założyć, że protokołem, z którego będą korzystać lokalne sieci państw członkowskich, będzie protokół TCP/IP. Niemniej jednak niektóre miejsca będą bazowały na wersji 4, podczas gdy inne na wersji 6. Punkty dostępu do sieci muszą oferować możliwość pełnienia roli bramy (ang. *gateway*) i muszą być w stanie działać niezależnie od protokołów sieciowych używanych w głównym SIS II, a także w N.SIS II.

4.6.3. Dodanie statycznej trasy

CU i BCU mogą korzystać z jednego, identycznego adresu IP w celu łączenia się z państwami członkowskimi. W związku z tym infrastruktura komunikacyjna powinna obsługiwać dodanie statycznej trasy (ang. *Static Route Injection*).

4.6.4. Utrzymane przepustowości

Tak długo jak połączenie CU lub BCU ma obciążenie mniejsze niż 90 %, dane państwo członkowskie musi być w stanie utrzymywać stale 100 % przypisanej mu szerokości pasma.

4.6.5. Inne wymogi

Aby obsługiwać CS-SIS, infrastruktura komunikacyjna musi spełniać przynajmniej minimalne wymogi techniczne.

Opóźnienie przejścia (ang. *transit delay*) musi być (włączając godziny największego ruchu) niższe lub równe 150 ms w 95 % pakietów oraz niższe niż 200 ms w 100 % pakietów.

Prawdopodobieństwo utraty pakietów musi być (włączając godziny największego ruchu) niższe lub równe 10^{-4} w 95 % pakietów oraz niższe niż 10^{-3} w 100 % pakietów.

Wyżej wymienione wymogi należy rozpatrywać osobno dla każdego punktu dostępowego.

Połączenie pomiędzy CU i BCU musi mieć opóźnienie (ang. *Round Trip Delay*) niższe lub równe 60 ms.

4.7. *Niezawodność systemu*

Przy projektowaniu CS-SIS jako wymóg postawiono sobie wysoką dostępność systemu. W związku z tym system jest odporny na wadliwe działanie części składowych dzięki podwojeniu wszystkich elementów wyposażenia.

Części składowe infrastruktury komunikacyjnej również muszą być odporne na wadliwe działanie poszczególnych elementów. Z punktu widzenia infrastruktury komunikacyjnej oznacza to, że niezawodne muszą być następujące części składowe:

— sieć szkieletowa,

— urządzenia trasujące,

— punkty dostępu do Internetu typu POP (ang. *Points of Presence*),

— podłączenia pętli lokalnej (ang. *Local loop connections*) (w tym fizycznie redundantne okablowanie),

— urządzenia zabezpieczające (urządzenia szyfrujące, zapory itp.),

— wszystkie usługi ogólne (DNS, NTP itp.),

— LNI/BLNI.

Mechanizmy przejmowania funkcji w przypadku awarii, przewidziane dla całego sprzętu sieciowego, powinny uruchamiać się bez konieczności interwencji ręcznej.

5. **Monitoring**

Aby ułatwić monitoring, musi istnieć możliwość zintegrowania monitorujących narzędzi infrastruktury komunikacyjnej z instrumentami monitoringu organu odpowiedzialnego za zarządzanie operacyjne głównym SIS II.

6. **Usługi ogólne**

Oprócz wyspecjalizowanych usług sieciowych i usług z zakresu bezpieczeństwa infrastruktura komunikacyjna musi także oferować usługi ogólne.

Usługi wyspecjalizowane muszą być wykonywane w obu jednostkach centralnych, aby uzyskać efekt redundancji.

Infrastruktura komunikacyjna musi oferować następujące fakultatywne usługi ogólne:

Usługa	Informacje dodatkowe
DNS	Obecnie procedura przejmowania funkcji w przypadku awarii, wiążąca się z przełączaniem się z CU na BCU w przypadku awarii sieci, oparta jest na zmianie adresu IP w ogólnym serwerze DNS.
Przekazywanie poczty elektronicznej	Korzystanie z ogólnej usługi przekazywania poczty elektronicznej może przydać się do normalizowania ustawień poczty elektronicznej dla różnych państw członkowskich oraz, przeciwnie niż ma to miejsce w przypadku serwera wyspecjalizowanego, nie zużywa żadnych zasobów sieciowych z CU/BCU. Wiadomości elektroniczne korzystające z ogólnej usługi przekazywania poczty elektronicznej muszą pozostać zgodne ze swoim szablonem bezpieczeństwa (ang. *security template*).
NTP	Usługa ta może być stosowana do synchronizacji zegarów w sprzęcie sieciowym.

7. **Dostępność**

CS-SIS oraz LNI i BLNI muszą być w stanie zapewnić nieprzerwaną dostępność na poziomie 99,99 % przez okres 28 dni, nie włączając w to dostępności sieci.

Infrastrukturę komunikacyjną musi cechować dostępność na poziomie 99,99 %.

8. **Usługi z zakresu bezpieczeństwa**

8.1. *Szyfrowanie sieci*

Główny SIS II nie pozwala na przesył danych o wysokim lub bardzo wysokim poziomie zabezpieczenia poza sieć LAN, jeśli nie zostaną zaszyfrowane. Należy uniemożliwić dostawcy sieci uzyskanie w jakikolwiek sposób dostępu do danych operacyjnych SIS II, a także do powiązanej z nimi wymiany danych między biurami SIRENE.

Aby utrzymać wysoki poziom bezpieczeństwa, infrastruktura komunikacyjna musi umożliwiać posługiwanie się certyfikatami lub kluczami. Należy umożliwić zarządzanie urządzeniami szyfrującymi na odległość i ich monitorowanie na odległość. Algorytmy szyfrujące muszą spełniać przynajmniej następujące wymogi:

— symetryczne algorytmy szyfrujące:

  • 3DES (128 bitów) lub lepsze,

  • wygenerowanie klucza zależy od wartości losowej, która nie pozwala na redukcję przestrzeni kluczy przy próbie wtargnięcia,

  • klucze lub informacje szyfrujące, które mogą zostać wykorzystane do przekazania kluczy, są zawsze chronione podczas ich przechowywania w pamięci,

— asymetryczne algorytmy szyfrujące:

  • RSA (moduł 1 024-bitowy) lub lepsze,

  • wygenerowanie klucza zależy od wartości losowej, która nie pozwala na redukcję przestrzeni kluczy przy próbie wtargnięcia.

Wykorzystywany będzie protokół *Encapsulated Security Payload* (ESP, RFC2406) w trybie tunelowym. Ładunek i oryginalny nagłówek protokołu IP i zostaną zaszyfrowane.

Do wymiany kluczy sesji stosowany będzie protokół wymiany kluczy internetowych IKE (ang. *Internet Key Exchange*).

Klucze IKE zachowają ważność nie dłużej niż jeden dzień.

Klucze sesji zachowają ważność nie dłużej niż jedną godzinę.

8.2. *Inne zabezpieczenia*

Infrastruktura komunikacyjna musi chronić nie tylko punkty dostępowe SIS II, ale także fakultatywne usługi ogólne. Usługi te muszą spełniać te same wymogi bezpieczeństwa co w CS-SIS. Wszystkie usługi ogólne muszą w związku z tym co najmniej być chronione przez zaporę sieciową, program antywirusowy i system wykrywania włamań IDS (ang. *Intrusion Detection System*). Ponadto urządzenia przeznaczone do usług ogólnych i ich zabezpieczenia powinny być pod stałym nadzorem zabezpieczającym (rejestracja danych i dalsze działania).

Aby zachować wysoki poziom bezpieczeństwa, organ odpowiedzialny za zarządzanie operacyjne głównym SIS II musi wiedzieć o wszelkich przypadkach naruszenia zabezpieczeń, które mają miejsce w infrastrukturze komunikacyjnej. W związku z tym infrastruktura komunikacyjna musi umożliwiać bezzwłoczne zgłaszanie takich przypadków organowi odpowiedzialnemu za zarządzanie operacyjne głównym SIS II. Wszystkie tego rodzaju przypadki muszą być zgłaszane regularnie, tzn. raz na miesiąc i w momencie ich stwierdzenia.

9. **Dział pomocy technicznej i struktura wsparcia**

Operator infrastruktury komunikacyjnej musi zapewniać funkcjonowanie działu pomocy technicznej, który pozostaje w kontakcie z organem odpowiedzialnym za zarządzanie operacyjne głównym SIS II.

10. **Współdziałanie z innymi systemami**

Infrastruktura komunikacyjna musi zapobiegać wydostawaniu się informacji z przypisanych im kanałów komunikacyjnych. Z punktu widzenia realizacji technicznej oznacza to, że:

— wszelki nieupoważniony lub niekontrolowany dostęp do innych sieci jest ściśle zabroniony; dotyczy to również połączeń z Internetem,

— nie może mieć miejsca przeciek danych do innych systemów w sieci; np. niedozwolone jest łączenie różnych IP VPN.

Oprócz wymienionych ograniczeń technicznych ma to również wpływ na działalność działu pomocy technicznej infrastruktury komunikacyjnej. Dział pomocy technicznej nie może ujawniać żadnych informacji odnoszących się do głównego SIS II żadnej stronie oprócz strony odpowiedzialnej za zarządzanie operacyjne głównym SIS II.