РЕШЕНИЕ НА СЪВЕТА

от 31 март 1992 година

в областта на сигурността на информационните системи

(92/242/ЕИО)

СЪВЕТЪТ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската икономическа общност, и по-специално член 235 от него,

като взе предвид предложението на Комисията[1],

като взе предвид становището на Европейския парламент[2],

като взе предвид становището на Икономическия и социален комитет[3],

като има предвид, че мисията на Общността е, чрез установяването на общ пазар и чрез постепенното сближаване на икономическите политики на държавите-членки, да се стимулира хармонично развитие на икономическите дейности в цялата Общност, непрекъснато и равномерно разширяване, увеличаване на стабилността, ускорено повишаване на стандарта на живот и по-тесни връзки между държавите-членки;

като има предвид, че информацията съхранявана, обработвана и предавана с помощта на електронни средства придобива все по-голямо значение в икономическата и социалната дейност;

като има предвид, че въвеждането на ефективни глобални съобщения и на разширяващото се използване на електронната обработка на информацията постави по-силно ударението върху необходимостта от подходяща защита;

като има предвид, че в своите дебати и резолюции, Европейският парламент на няколко пъти подчерта значението на сигурността на информационните системи;

като има предвид, че Икономическият и социален комитет подчерта необходимостта да се разглеждат въпросите, свързани със сигурността на информационните системи във видовете дейности на Общността, особено с оглед на въздействието на завършването на вътрешния пазар;

като има предвид, че действията на национално, международно равнище и на равнище на Общността осигуряват една добра основа;

като има предвид, че има тясна връзка между далекосъобщенията, информационните технологии, стандартизацията, пазара на информацията и

[1] ОВ C 277, 5.11.1990 г., стр. 18.
[2] ОВ C 94, 13.3.1992 г.
[3] ОВ C 159, 17.6.1991 г., стр. 38.

политиките на изследователската и технологичната развойна дейност (ТРД), както и с вече предприетата от Общността работа в тази област;

като има предвид, че е подходящо да се съгласуват усилията, като се използват за основа съществуващите на национално и международно ниво разработки и като се насърчава сътрудничеството между главните заинтересувани страни; като има предвид, че поради това е подходящо да се направят стъпки в рамките на един съгласуван план за действие;

като има предвид, че сложността на сигурността на информационните системи изисква създаването на стратегии, даващи възможност информацията да се разпространява свободно в рамките на единния пазар, като същевременно бъде гарантирана сигурността на използването на информационните системи в цялата Общност;

като има предвид, че отговорност на всяка държава-членка е да се съобразява с ограниченията, наложени от сигурността и обществения ред;

като има предвид, че отговорностите на държавите-членки в тази област предполагат един съгласуван подход, основан на тясно сътрудничество с висши държавни служители на държавите-членки;

като има предвид, че следва да се предвиди план за действие за първоначален период от двадесет и четири месеца и създаването на комитет на висшите държавни служители, с дългосрочен мандат, които да съветват Комисията относно действията в областта на сигурността на информационните системи;

като има предвид, че сума в размер на 12 милиона екю се счита за необходима за осъществяването на действието за първоначален период от двадесет и четири месеца; като има предвид, че за 1992 година, в рамките на актуалните финансови прогнози, сумата, която се смята за необходима е 2 милиона екю;

като има предвид, че сумите, които трябва да се вложат с оглед финансирането на програмата за периода след бюджетната 1992 година ще образува част от съществуващата финансова рамка на Общността;

РЕШИ:

Член 1

С настоящото решение се приема действие в областта на сигурността на информационните системи. То включва:

- развитието на глобални стратегии за гарантиране на сигурността на информационните системи (план за действие) за първоначален период от двадесет и четири месеца,

и

- създаването на група от висши държавни служители, на които е предоставен дългосрочен мандат, по-долу наричана „комитет”, с цел да съветва Комисията

относно действията, които трябва да бъдат предприемани в областта на сигурността на информационните системи.

Член 2

1. Комисията се консултира редовно с комитета по въпросите, имащи връзка със сигурността на информационните системи за различните дейности, осъществявани от Общността, по-специално за определянето на работни стратегии и програми.

2. Както е посочено в приложението, планът за действие включва подготвителната работа, отнасящи се до следните теми:

I. развитие на стратегическа рамка за сигурността на информационните системи;

II. определяне на нуждите на потребителите и на доставчиците на услуги в областта на сигурността на информационните системи;

III. изготвяне на решения за някои краткосрочни и средносрочни нужди на потребителите, на доставчиците и на доставчиците на услуги;

IV. разработване на спецификации, стандартизация, оценка и сертифициране относно сигурността на информационните системи;

V. технологично и оперативно развитие в областта на сигурността на информационните системи;

VI. реализиране на сигурността на информационните системи.

Член 3

1. Размерът на финансирането от страна на Общността, оценено като необходимо за осъществяване на дейността е 12 милиона екю за първоначалния период, от които 2 милиона екю за 1992 година, в рамките на финансовата перспектива за периода 1988 - 1992 г.

За следващия период на прилагане на програмата сумата ще трябва да се включи в действащата финансова рамка на Общността.

2. Бюджетният орган определя наличните финансови средства за всяка финансова година, като се съобразява с принципите на доброто управление, посочени в член 2 от Финансовия правилник, приложим по отношение на общия бюджет на Европейските общности.

Член 4

Група от независими експерти осъществява, за нуждите на Комисията, оценка на постигнатия напредък през първоначалния период. Докладът на тази група, придружен от евентуалните забележки на Комисията се представя на Европейския парламент и на Съвета.

Член 5

1. Комисията отговаря за въвеждането на плана за действие. Тя се подпомага от Консултативен комитет, съставен от представители на държавите-членки и председателстван от представителя на Комисията.

2. Планът за действие се привежда в изпълнение в съответствие с целите, определени в член 2 и той се актуализира, когато това е необходимо. Той излага подробно целите и видовете дейности, които трябва да се предприемат, както и свързаните с това финансови договорености. Комисията отправя покана за участие с предложения въз основа на плана за действие.

3. Планът за действие се изпълнява в тясно сътрудничество с действащите лица в този сектор. Той отчита, развива и допълва дейностите по стандартизацията, които се извършват в момента на европейско и международно равнище в тази област.

Член 6

1. Процедурата, предвидена в член 7 се прилага по отношение на мерките, свързани с политиката на Общността в областта на сигурността на информационните системи.

2. Процедурата, предвидена в член 8 се прилага:

- при изработването и актуализирането на плана за действие, посочен в член 5,

- по отношение на съдържанието на поканите за участие с предложения, на оценяването на предложенията и по отношение на разглеждания размер на участието на Общността в мерките, когато то надхвърля ECU 200 000;

- по отношение на сътрудничеството на организации извън Общността, във всяка дейност, извършвана по силата на настоящото решение;

- по отношение на реда за разпространение, защита и оценяване на резултатите от взетите мерки,

- по отношение на мерките, които трябва да бъдат взети, за да се оцени дейността.

3. Когато размерът на участието на Общността в осъществяването на мерките е по-нисък или равен на ECU 200 000, Комисията се консултира комитета за мерките, които трябва да бъдат взети и съобщава за резултата от своята оценка.

Член 7

Представителят на Комисията представя на комитета проект за мерките, които трябва да бъдат взети. Комитетът излиза със становище по този проект в срок, който председателят може да определи в зависимост от спешността на разглеждания въпрос, когато това е необходимо, като пристъпи към гласуване.

Становището се отразява в протокола; освен това, всяка държава-членка има право да иска нейното становище да бъде вписано в протокола.

Комисията се съобразява възможно най-много със становището, дадено от комитета. Тя информира комитета за начина, по който тя се е съобразила с това становище.

Член 8

Представителят на Комисията представя на комитета проект за мерките, които трябва да бъдат взети. Комитетът излиза със становище по този проект в срок, който председателят може да определи в зависимост от спешността на разглеждания въпрос. Становището се приема с мнозинството, предвидено в член 148, параграф 2 от Договора, за взимане на решенията, които Съветът е призван да взема по предложение на Комисията. При гласуванията в комитета, гласовете на представителите на държавите-членки се претеглят по начина, определен в посочения по-горе член. Председателят не гласува.

Комисията приема предвидените мерки, когато те съответстват на становището на комитета.

Когато предвидените мерки не съответстват на становището на комитета, или при липса на становище, Комисията представя незабавно на Съвета предложение относно мерките, които трябва да се вземат. Съветът взима решение с квалифицирано мнозинство.

Ако, при изтичането на срок от три месеца, считано от датата на сезиране на Съвета, той не се е произнесъл, предложените мерки се приемат от Комисията, освен в случая, когато Съветът се е произнесъл с обикновено мнозинство срещу цитираните мерки.

Съставено в Брюксел на 31 март 1992 година.

За Съвета:
Председател
Vitor MARTINS

ПРИЛОЖЕНИЕ

Резюме на насоките на действие

НАСОКИ ЗА ПЛАН ЗА ДЕЙСТВИЕ В ОБЛАСТТА НА СИУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

ВЪВЕДЕНИЕ

Планът за действие има за цел да развие глобалните стратегии, целящи да доставят на потребителите и на създателите на информация, съхранявана, обработвана или предавана в електронен вид с подходяща защита на информационните системи срещу случайните или целенасочени заплахи.

Планът за действие взима предвид и допълва дейностите по стандартизацията, осъществявани в момента в тази област на световно равнище.

Той включва следните насоки на дейност:

- развитието на една стратегическа рамка за сигурността на информационните системи,

- установяване на нуждите на потребителите и на доставчиците на услуги в областта на сигурността на информационните системи,

- изработване на решения за някои краткосрочни и средносрочни потребности на потребителите, на доставчиците и на доставчиците на услуги,

- изработване на спецификации, стандартизация, оценяване и сертифициране относно сигурността на информационните системи,

- технологични и оперативни разработки в областта на сигурността на информационните системи,

- осъществяване на сигурността на информационните системи.

Планът за действие се осъществява от Комисията, в тясно сътрудничество със свързаните дейности в държавите-членки и във връзка с изследователските и развойните дейности на Общността в тази област.

1. НАСОКА НА ДЕЙСТВИЕ I: РАЗВИТИЕ НА СТРАТЕГИЧЕСКА РАМКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

1. 1. Проблемът

Сигурността на информационните системи е призната като качество, необходимо навсякъде в модерното общество. Електронните информационни услуги изискват сигурни далекосъобщителни инфраструктури, защитен хардуер и софтуер, както и сигурни условия за използване и управление. Трябва да се изработи глобална стратегия, отчитаща всички аспекти на сигурността на

информационните системи, като се избягва всякакъв фрагментарен подход. Всяка стратегия за сигурността на електронно обработваната информация трябва да отразява желанието на всяко общество да действа ефективно, като същевременно се предпазва в един бързопроменящ се свят.

1. 2. Целта

Трябва да бъде създадена стратегическа рамка, за да се съгласуват социалните, икономическите и политическите цели с техническите, оперативни и правни решения на Общността в международен контекст. Участващите в тази сфера са тези, които като работят заедно за развитието на общо виждане и на договорена стратегическа рамка, трябва да постигнат деликатно равновесие между различните грижи, цели и ограничения. Става въпрос за едно предварително действие, което да примири интересите и потребностите, както в областта на воденето на дадена политика, така и на промишленото развитие.

1. 3. Статут и тенденции

Ситуацията се характеризира с нарастващо осъзнаване на необходимостта да се предприемат действия. Независимо от това, при липсата на инициатива за съгласуване на усилията, е много възможно усилията, разпръснати в разнообразни сектори, да доведат до фактически противоречива ситуация, като създават постепенно все повече сериозни правни, социални и икономически проблеми.

1. 4. Изисквания, възможности и приоритети

Една такава рамка би трябвало да има за предмет и да изследва анализа и управлението на риска в областта на уязвимостта на информационните системи и свързаните с тях услуги, хармонизирането на законовите и подзаконовите разпоредби относно злоупотребата с компютри/далекосъобщения, административните инфраструктури, включително политиката на сигурността и как тя може да бъде ефективно осъществена посредством различни видове дейности/ дисциплини, социалните проблеми и тези за защита на личния живот (например прилагане на системи за идентифициране, за установяване на самоличност, за недопускане на отхвърляне и, евентуално, за даване на разрешение в една демократична среда).

Трябва да бъдат дадени ясни насоки, за да бъдат създадени физически и логически конструкции за разпространение на сигурни информационни услуги, стандарти, ръководни насоки и определения за продуктите и услугите с гарантирана сигурност, пилотни проекти и прототипи, за да бъде гарантирана жизнеспособността на различните административни структури, както и конструкции и норми отнасящи се до нуждите на специфични сектори.
Трябва да бъде насърчавано осъзнаването на проблемите на сигурността, по такъв начин, че да бъдат подтикнати потребителите да демонстрират повишена загриженост за сигурността в областта на информационните технологии (ИТ).

2. НАСОКА НА ДЕЙСТВИЕ II: УСТАНОВЯВАНЕ НА ИЗИСКВАНИЯТА ЗА ПОТРЕБИТЕЛИТЕ И ДОСТАВЧИЦИТЕ НА УСЛУГИ В ОБЛАСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ.

2. 1. Проблемът

Сигурността на информационните системи е вътрешно присъщото условие на цялостта и на надеждността на търговските приложения, на интелектуалната собственост и на поверителността. Това поставя проблема за деликатното равновесие и понякога за избора между, от една страна, ангажимента към свободната търговия и, от друга страна, защитата на личната сфера и на интелектуалната собственост. Тези избор и компромиси трябва да бъдат направени на основата на общата преценка на изискванията и на въздействието на възприетите варианти в областта на сигурността на информационните системи, за да се отговори на тези потребности.

Изискванията за потребителите обхващат функции по сигурността на информационните системи, свързани с технологичните, оперативните и административните аспекти. Ето защо системна изследователска дейност на изискванията във връзка със сигурността на информационните системи формира съществена част от изработването на подходящи и ефикасни мерки.

2. 2. Цел

Установяване естеството и характеристиките на изискванията на потребителите и на доставчиците на услуги и тяхното отношение към мерките в областта на сигурността на информационните системи.

2. 3. Статут и тенденции

До момента не са били положени никакви съгласувани усилия за определяне на бързо развиващите и променящи се потребности на главните действащи лица в сферата на сигурността на информационните системи. Някои държави-членки и Общността са установили необходимостта от хармонизиране на националните действия (особено на „критериите за оценяване на сигурността на ИТ”). От най-голямо значение са еднаквите критерии и правила за взаимното признаване на сертификатите от оценяването.

2. 4. Изисквания, възможности и приоритети

За да бъдат разглеждани оправданите потребности на действащите лица в сектора по съгласуван и прозрачен начин, се счита за необходимо да се изработи утвърдена класификация на потребностите на потребителите и на тяхната връзка с осъществяването на сигурността на информационните системи.

Важно е също така да се установят изискванията в областта на законовите, подзаконови разпоредби и кодексите за поведение в светлината на една оценка на тенденциите относно характерните особености и технологията на услугите, за да се определят други стратегии, даващи възможност да се постигнат целите посредством административни, служебни, оперативни и технически разпоредби и да се оцени ефективността и достъпността и цената на различните решения и на резервните стратегии в областта на сигурността на информационните системи за потребителите, доставчиците на услуги и операторите.

3. НАСОКА НА ДЕЙСТВИЕ III: ИЗГОТВЯНЕ НА РЕШЕНИЯ ЗА НЯКОИ КРАТКОСРОЧНИ И СРЕДНОСРОЧНИ ПОТРЕБНОСТИ НА

ПОТРЕБИТЕЛИТЕ, НА ДОСТАВЧИЦИТЕ И НА ДОСТАВЧИЦИТЕ НА УСЛИГИ

3. 1. Проблемът

Днес е възможно компютрите да се защитават от неразрешения достъп от външния свят посредством мерки за „изолиране", т. е. чрез прилагане на традиционни, в организационен и физически аспект, мерки. Това се отнася и за електронните съобщения в рамките на една затворена група потребители, действащи в една затворена мрежа. Положението е съвсем различно, когато информацията се споделя от различни групи потребители или се обменя чрез обществена или общодостъпна мрежа. Технологията, терминалите и услугите от една страна, и свързаните стандарти и процедури, от друга страна, обикновено не са в състояние, в такива случаи, да гарантират сигурност на информационните системи на подобно ниво.

3. 2. Цел

Целта трябва да бъде да се дадат, в кратки срокове, решения, които могат да отговорят на най-непосредствените потребности на потребителите, на доставчиците на услуги и на производителите. Това предполага използването на общи критерии за оценяване на сигурността на ИТ. Тези критерии трябва да бъдат създадени така, че да бъдат отворени за бъдещите изисквания и решения.

3. 3. Статут и тенденции

Някои групи потребители са създали, за тяхно собствено ползване, техники и процедури, отговарящи специално на целите на разпознаването, цялостта и неотхвърлянето. Обикновено се използват магнитни карти или карти с памет. Някои използват шифровъчни техники с различна сложност. Често това налага определянето на специални „инстанции" за групите потребители. Трудно е обаче да се масовизарат тези техники и методи, за да се отговори на потребностите в една достъпна среда.

ISO работи върху системата на сигурност на информационните системи OSI (ISDKDIS 7498-2), както и CCITT в контекста на X 400. Възможно е също да се вмъкнат сегменти за сигурност в съобщенията. Разпознаването, цялостта и неотхвърлянето се разглеждат като част от съобщенията (EDIFACT), както и от X 400 MHS.

В настоящия момент, правната рамка на EDI (Electronic Data Interchange) е все още на ниво обмисляне. Международната търговска камара публикува единни правила за поведение за размяната на търговски сведения през далекосъобщителните мрежи.

Няколко държави (например Германия, Франция, Обединеното кралство и Съединените американски щати) са създали или изработват критерии за оценяване надеждността на информационните технологии и на далекосъобщителните продукти и системи и на съответните процедури, за да се пристъпи към оценяването. Тези критерии са били съгласувани с националните производители и те ще доведат до увеличаване броя на надеждните изделия и системи, като се започне от простите продукти. Създаването на национални

организации, натоварени с провеждането на оценяване и с предоставянето на сертификати, ще бъде в подкрепа на тази тенденция.

По голямата част от потребителите смятат, че разпоредбите в областта на поверителността имат по-малко значение. Възможно е все пак ситуацията да се промени в бъдеще, поради все по-широкото разпространение на съвременни съобщителни услуги и особено на мобилните услуги.

3. 4. Изисквания, възможности и приоритети

От основно значение е да се развиват веднага щом бъде възможно, процедурите, стандартите, продуктите и инструментите, годни да гарантират сигурността на информационните системи като такива (компютри, периферия) и на публичните съобщителни мрежи. Висок приоритет би трябвало да бъде отдаден на разпознаването, цялостта и неотхвърлянето. Би следвало да се разработят пилотни проекти за да се установи годността на предлаганите разрешения. Решенията за някои приоритетни потребности в областта на EDI се търсят в рамките на програмата TEDIS и се координират в по-широкия контекст на настоящия план за действие.

4. НАСОКА НА ДЕЙСТВИЕ IV: ИЗРАБОТВАНЕ НА СПЕЦИФИКАЦИИ, СТАНДАРТИЗАЦИЯ, ОЦЕНЯВАНЕ И СЕРТИФИЦИРАНЕ ВЪВ ВРЪЗКА СЪС СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

4. 1. Проблемът

Изискванията в областта на сигурността на информационните системи са широко разпространени и поради това съществуването на общи спецификации и стандарти е решаващо. Липсата на утвърдени стандарти и спецификации за сигурността на информационните технологии би могла да представлява голяма пречка за напредъка на процесите и услугите, основани на информацията, навсякъде в икономиката и в обществото.

Трябва също да се вземат мерки за ускоряването на изготвянето и използването на технология и на стандарти в няколко области, свързани с комуникациите и с компютърните мрежи, които са от основно значение за потребителите, за промишлеността и за администрацията.

4. 2. Цел

Необходими са усилия, за да се предоставят средства за поддържане и осъществяване на специфични функции по сигурността в общите области на OSI, на ONP, на RNIS/IBC и на управлението на мрежите. Техниките и подходите в областта на проверяването, включително и сертифицирането, които водят до взаимно признаване, са свързани, по своята вътрешна същност, със стандартизацията и със спецификацията. Винаги когато това е възможно, трябва да се подкрепят решения, приети на международно равнище. Би трябвало също да се насърчава развитието и използването на информационни системи, снабдени със защитни функции.

4. 3. Статут и тенденции

Съединените американски щати, по-специално, са предприели основни инициативи, за да бъде разгледан въпросът за сигурността на информационните системи. В Европа, този проблем се разглежда в контекста на ИТ и стандартизацията на далекосъобщенията в рамките на ETSI и на CEN/Cenelec, при подготовка на работата на CCITT и на ISO в тази област. Поради нарастващата загриженост, работата в Съединените американски щати се интензифицира бързо и както продавачите, така и доставчиците на услуги увеличават усилията си в тази област. В Европа, Франция, Германия и Обединеното кралство, започнаха независимо една от друга сходни дейности, но общо усилие, отговарящо на това на Съединените американски щати, се развива бавно.

4. 4. Изисквания, възможности и приоритети

В областта на сигурността на информационните системи нормативната уредба, оперативните, административните и техническите аспекти, са по същество много тясно свързани. Правните разпоредби трябва да бъдат отразени в стандартите и разпоредбите в областта на сигурността на информационните системи следва да бъдат съобразени със стандартите и разпоредбите по начин, подлежащ на проверка. В няколко аспекта разпоредбите трябва да съдържат спецификации, надхвърлящи традиционния обхват на стандартизацията, т. е. включващи кодекси за поведение. Изисквания по отношение на стандартите и кодексите за поведение съществуват във всички сектори на сигурността на информационните системи и трябва да се разграничат изискванията за защита, отговарящи на целите в областта на сигурността и някои от техническите изисквания, които могат да бъдат поверени на компетентните европейски органи по стандартизация (CEN/Cenelec/ETSI).

Спецификациите и стандартите трябва да обхващат материята на услугите по сигурността на информационните системи (проверка самоличността на лицата и на предприятията, протоколи за не-отхвърляне, правно валидно електронно доказателство, контрол за разпознаване), техните съобщителни услуги (защита на личния живот от гледна точка на разпространението на образ, на глас и на данни, защита на базите с изображения и с данни, сигурност на свързаните услуги), тяхното управление на комуникациите и на сигурността (система на публични/частни ключове за функционирането на откритите мрежи, за защита на управлението на мрежите, защитата на доставчиците на услуги) и тяхното сертифициране (критерии и нива на осигуряване, процедури на осигуряването на сигурността на информационните системи).

5. НАСОКА ЗА ДЕЙСТВИЕ V: ТЕХНОЛОГИЧНО И ОПЕРАТИВНО РАЗВИТИЕ В ОБЛАСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

5. 1. Проблемът

Системна изследователска и развойна технологична дейност, даваща възможност да се намерят икономически пригодни и оперативно задоволителни отговори на една серия от настоящи и бъдещи изисквания в областта на сигурността на информационните системи е необходимо условие за развитието на пазара на услугите и за конкурентоспособността на европейската икономика в нейната цялост.

Всяко технологично развитие в областта на сигурността на информационните системи ще трябва да отразява едновременно сигурността в областта на информатиката и сигурността на съобщенията, доколкото повечето от сегашните системи са разпространени системи, достъпът до които се осъществява чрез съобщителни услуги.

5. 2. Цел

Системна изследователска и развойна технологична дейност, даваща възможност да се намерят икономически пригодни и оперативно задоволителни отговори на една серия от настоящи и бъдещи изисквания в областта на сигурността на информационните системи.

5. 3. Изисквания, възможности и приоритети

Разработките в областта на сигурността на информационните системи би трябвало да са насочени към стратегиите на развитието и на реализацията, към технологиите, както и към интеграцията и проверяването.

Стратегическата изследователска и насочена към технологично развитие дейност трябва да включва изучаването на концептуални модели на сигурни системи (сигурни от гледна точка на неразрешени изменения и на отказ на услуга), на модели на функционални изисквания, на модели на риска и на структури за сигурността.

Изследователската и развойна технологична дейност би трябвало да включва разпознаването на потребителя и на съобщението (например благодарение на анализа на гласа и на електронните подписи), техническите интерфейси и протоколите за шифроване, механизмите за контрол на достъпа и методите за прилагане, за постигане на доказуемо сигурни системи.

Проверката и валидирането на сигурността на техническата система и нейната приложимост биха били разгледани посредством проекти за интеграция и за проверка.

Освен консолидирането и развитието на технологията на сигурността, определен брой поддържащи мерки са необходими в областта на създаването, поддръжката и съгласуваното прилагане на стандартите, както и на валидирането и сертифицирането на изделията на ИТ що се отнася до техните качества в областта на сигурността, включително валидирането и сертифицирането на методите на проектиране и прилагане на системите.

Третата рамкова програма на Общността за изследователска и технологична развойна дейност би могла да се използва за подпомагане на проекти за сътрудничество на предконкурентно и преднормативно ниво.

6. НАСОКА ЗА ДЕЙСТВИЕ VI: ОСЪЩЕСТВЯВАНЕ НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

6. 1. Проблемът

В зависимост от конкретното естество на елементите за сигурността на информационните системи, ще трябва да се интегрират функциите, необходими в различни точки на информационната система, като се започне от терминалите/компютрите, услугите, управлението на мрежите и се стигне до шифровъчните устройства, до картите с памет, до публичните и частните ключове и т. н. Някои от тези функции вероятно ще бъдат включени в хардуера или софтуера, доставяни от продавачите, докато други могат или да бъдат част от разпределените системи (например управление на мрежи), или да бъдат притежание на индивидуални потребители (например карти с памет), или да бъдат доставяни от една специализирана институция (например публични и частни ключове).

По-голямата част от продуктите и услугите за сигурността вероятно може да бъдат доставяни от продавачи, доставчици на услуги или оператори. За някои специфични функции, като например доставката на публични/частни ключове, разрешението за одит е възможно да бъде необходимо да се определят и да се упълномощят подходящи организации.

Същото се отнася и за сертифицирането, оценката и проверяването на качеството на услугата, които са функции, които трябва да бъдат поверени на независими от интересите на продавачите, доставчиците на услуги или на операторите структури. Такива структури биха могли да бъдат или частни, или държавни, или упълномощени от държавата да изпълняват делегираните им функции.

6. 2. Цел

По начин, който да улесни хармоничното реализиране на сигурността на информационните системи в Общността с оглед предпазване на обществото и на търговските интереси, ще бъде необходимо да се възприеме съгласуван подход в областта на реализиране на сигурността на информационните системи. Когато на независими организации бъде възложен мандат, техните функции и условията за функционирането им ще трябва да бъдат определени и приети и, ако е необходимо вписани в съответствие с нормативната рамка. Целта ще бъде да се достигне, като предварително условие на взаимното признаване, до ясно определено разпределяне на отговорностите, договорено между различните участници на ниво на Общността.

6. 3. Положение и тенденции

Към момента, реализирането на сигурността на информационните системи е добре организирано само за отделни области и отговаря само на техните специфични потребности. Организацията на европейско ниво най-често е неформална и взаимното признаване на проверяването и на сертифицирането не се осъществява извън някои затворени групи. Поради нарастващото значение на сигурността на информационните системи, става спешно да се определи един съгласуван подход в тази област в Европа и на международно равнище.

6. 4. Изисквания, възможности и приоритети

Поради броя на различните заинтересовани участници и тесните връзки с въпросите на законовата и подзаконова уредба, особено е важно да се постигне

предварителна договореност относно принципите, които би трябвало да ръководят осъществяването на сигурността на информационните системи.

При определянето на едно последователно отношение в тази област, ще трябва да се разгледат аспектите на идентифицирането и на спецификацията на функциите, изискващи, поради самото тяхно естество, намесата на независими организации (или на организации, работещи съвместно). Това би могло да обхване такива функции като администрирането на система от публични/частни ключове.

Освен това, изисква се да се определят и да се уточнят на ранен етап функциите, които трябва, в обществен интерес да бъдат поверени на независими организации (или на организации, работещи съвместно). Тези функции биха могли например да включват одита, гарантирането на качеството, проверяването, сертифицирането и сходни функции.