ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелердің қауіпсіздік негіздері
1-бөлім
Шолу

Информационная технология
ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ
Основы безопасности для открытых систем
Часть 1
Обзор

ҚР СТ ИСО/МЭК 10181-1-2008

(ИСО/ХЭК 10181-1:1996 «Ақпараттық технология Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. 1-бөлік Шолу», IDT)

Ресми басылым

Қазақстан Республикасының Индустрия және сауда министрлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ

Ашық жүйелердің қауіпсіздік негіздері

1-бөлім

Шолу

ҚР СТ ИСО/МЭК 10181-1-2008

(ИСО/ХЭК 10181-1:1996 «Ақпараттық технология Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. 1-бөлік Шолу», IDT)

Ресми басылым

Қазақстан Республикасының Индустрия және сауда министрлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитетінің 2008 жылғы 25 ақпандағы № 107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт Қазақстан Республикасының экономикасының қажеттілігін айқындаушы қосымша талаптары көлбеу қаріппен белгіленген «Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері: Шолу» («Information technology. Open Systems Interconnection. Security frameworks for open systems: Overview»), IDT, ИСО/ХЭК 10181-1:1996 халықаралық стандартына сәйкес келеді

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелердің қауіпсіздік негіздері
1-бөлім
Шолу

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт ашық жүйелер ортасында қауіпсіздік сервистерін қолдану міндеттерін шешу үшін арналған Қауіпсіздік негіздерін белгілейді. «Ашық жүйелер» термині деректер қоры, таратылған қосымшалар, таратылған ашық деректерді өңдеу және ашық жүйелердің өзара байланысы салалары түсініледі.

Қауіпсіздік негіздері деректер элементімен сияқты, қауіпсіздіктің өзгеше сервистерін алуға қолданылатын әрекеттердің (бірақ хаттамалардың элементтерімен емес) кезектілігін басқарады. Бұл қауіпсіздік сервистері жүйелердің өзара байланысатын объектілері сияқты, жүйелер арасындағы деректермен алмасу, сонымен қатар жүйелермен басқарылатын деректер ретінде қолданылуы мүмкін.

Қауіпсіздік негіздері келісілген терминологияны және қауіпсіздіктің нақты талаптары үшін әмбебап абстрактылы интерфейстерінің анықтамаларын ұсына отырып, одан әрі стандарттау базасы болып табылады. Сонымен қатар, олар осы талаптарды орындауға қолданылатын механизмдерді жіктейді.

Көбінесе бір қауіпсіздік сервисі басқа сервистерге байланысты, ал бұл қауіпсіздік жүйесінің кейбір жеке бөліктерінің бөлінуін қиындатады. Қауіпсіздік негіздері нақты қауіпсіздік сервистерімен байланысты, қауіпсіздік сервистерін ұсыну үшін қолданылатын механизмдер спектрін сипаттайды және сервистер мен механизмдер арасындағы өзара байланысты анықтайды. Осы механизмдердің сипаттамасы басқа қауіпсіздік сервисіне сүйенуі мүмкін және қауіпсіздік инфрақұрылымы бір қауіпсіздік сервисінің қалай басқа сервиспен қолданылатындығын сипаттайды.

Осы стандартта пайдаланылатын қауіпсіздіктің кейбір сервистері криптографиялық әдістерді қолдануға негізделеді. Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі және осы стандарттың қарастыру заты болып табылмайды.

Осы стандарт:

– Қауіпсіздік негіздерін ұйымдастыруды;

– Қауіпсіздік негіздерінің бірнеше бөлімдерінде қолданылатын қауіпсіздік түсінігін анықтауды;

– Негіздің басқа бөлімдерінде анықталған сервистер мен механизмдердің өзара байланысын белгілейді.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандартарға сілтемелер пайдаланылды:

ҚР СТ ИСО/МЭК 9798-2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Мәндерді сәйкестендіру тетіктері. 1-бөлік. Жалпы модель

ҚР СТ ИСО/МЭК 10181-2-2006 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. Сәйкестендіру негіздері.

ҚР СТ ИСО/МЭК 10181-3-2008 Ақпараттық технологиялар. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. Кіруді басқару негіздері

ҚР СТ ИСО/МЭК 11770-1:2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 1-бөлік. Кілттерді басқару негіздері

ГОСТ ИСО 7498-2-2002 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 2-бөлік. Ақпаратты қорғау архитектурасы.

ИСО/МЭК 7498-1-1994 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Негізгі эталондық үлгі. Негізгі үлгі.

ИСО/МЭК 9594-8-1995 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Анықтамалықтар: Сәйкестендіру негіздері

3 Терминдер мен анықтамалар

Осы стандартта *ИСО/МЭК 7498-1,* ГОСТ ИСО 7498-2 бойынша терминдер, сондай-ақ тиісті анықтамаларымен мынадай терминдер пайдаланылды:

3.1 Қауіпсіздік әкімшілігі (security administrator): Қауіпсіздік саясатын анықтауға немесе бір немесе бірнеше бөліктердің ендірілуіне жауап беретін тұлға

3.2 Асимметриялық криптографиялық алгоритм (asymmetric cryptographic algorithm): Шифрлеу және шифрді ашу барысында кілттері ерекшеленетін шифрлеу және тиісті шифрді ашу алгоритмі.

Ескертпе – Кейбір криптографиялық алгоритмдерде шифрді ашу немесе сандық қолтаңбаны генерациялау үшін бірнеше жабық кілттер талап етіледі.

3.3 Сөзсіз сенімді мән (unconditionally trusted entity): Анықталмай қауіпсіздік саясатын бұзуға қабілетті сенімді мән.

3.4 Қауіпсіздікті қалпына келтіру (security recovery): Егер қауіпсіздіктің бұзушылықтары анықталған болса немесе күмән тудырса, алдын ала қабылданатын әрекеттер мен орындалатын процедуралар.

3.5 Сенімді мән (trusted entity): Қауіпсіздік саясатын бұзатын немесе одан күтпеген әрекеттерді орындайтын немесе күтілетін әрекеттерді сәтсіз орындағандағы мән.

3.6 Сенімді үшінші тарап (trusted third party): Әрекеттердің қауіпсіздігімен (қауіпсіздік саясатының контекстінде) байланысты шектерде сенетін қауіпсіздік жөніндегі уәкілі немесе оның агенті.

3.7 Сенім (trust): X мәні кейбір әрекеттер жинағы шегінде және X мәні осы шектерде Y мәнінің тиісті әрекетіне сүйенген жағдайда Y мәніне сенеді дейді.

3.8 Қауіпсіздік домені (security domain): Элементтер жинағы, қауіпсіздік саясаты, қауіпсіздік жөніндегі уәкіл және элементтер жинағы берілген әрекеттер үшін қауіпсіздік саясатының субъектісі болып табылатын қауіпсіздікпен байланысты әрекеттер жинағы, ал қауіпсіздік саясатын осы қауіпсіздік домені жөніндегі уәкіл басқарады

3.9 Жабық кілт (private key): Қолданылуы шектеулі асимметриялық криптографиялық алгоритмде қолданылатын кілт (әдетте бір ғана мәнге қолданылады).

3.10 Қауіпсіздік ақпараты (security information): Қауіпсіздік сервистерін іске асыруға қажетті ақпарат.

3.11 Криптографиялық тіркеме (cryptographic chaining): Түрлену алгоритммен орындалатын криптографиялық алгоритмді пайдалану режимі, алдыңғы кіріс немесе шығыс деректерінің мәндеріне байланысты.

3.12 Қауіпсіздік маркері (security token): Бір немесе бірнеше қауіпсіздік сервистерімен мәндердің өзара байланысы арасында таратылатын қауіпсіздік сервистерінің деректерін ұсыну кезінде қолданылатын қауіпсіздік ақпаратымен бірге қорғалған деректер жинағы.

3.13 Бір тараптық функция (one-way function): Оңай есептелетін, бірақ нәтижесі белгілі болғанда осы нәтижені алуға қолданылатын қандай да бір мәннің табылуы қиын функция (математикалық).

3.14 Бір тараптық хэш-функция (one-way hash function): Біруақытта бір тараптық және хэш-функция болып табылатын функция (математикалық).

3.15 Ашық кілт (public key): Асимметриялық криптографиялық алгоритмде және жалпымен қолданылатын кілт.

3.16 Ерекше идентификатор (distinguishing identifier): Мәнді бірегей идентификациялайтын деректер.

3.17 Пломба (seal): Тұтастықты қамтамасыз ететін, бірақ алушымен жасандыдан қорғай алмайтын (яғни, істен шықпауын қамтамасыз ете алмайтын) криптографиялық бақылаулы мән. Егер 65

пломба деректер элементімен ассоциацияланса, онда бұл деректер элементі *пломбаланған* болып саналады.

Ескертпе – Дегенмен, пломбаның өзі істен шықпауды қамтамасыз етпегенімен, кейбір істен шықпау механизмдері пломбамен қамтамасыз етілетін тұтастық сервисін қолданады, мысалы, коммуникацияны қорғау үшін сенімді үшінші тарап әрекет етеді.

3.18 Қауіпсіз өзара байланысу ережесі (secure interaction rules): Қауіпсіздік домендері арасындағы өзара байланысты реттейтін қауіпсіздік саясатының ережелері.

3.19 Қауіпсіздік саясатының ережелері (security policy rules): Нақты жүйе шегінде қауіпсіздік домені үшін қауіпсіздік саясатын ұсыну.

3.20 Құпиялы кілт (secret key): Симметриялық криптографиялық алгоритмде қолданылатын кілт. Құпиялы кілттің қолданылуы шектелген (әдетте екі мәнге ғана қолданылады).

3.21 Қауіпсіздік сертификаты (security certificate): Қауіпсіздік жөніндегі уәкілмен немесе сенімді үшінші тараппен дереккөздерінің тұтастылық және сәйкестендіру сервистерін ұсыну үшін қолданылатын қауіпсіздік ақпаратымен қатар шығарылған деректердің қауіпсіздігімен байланысты жинақ.

Ескертпе – Барлық сертификаттар қауіпсіздік сертификаттары болып саналады (МСТ ИСО 7498-2:2002 тиісті анықтамаларды қараңыз). «қауіпсіздік сертификаты» термині ИСО/МЭК 9594-8 (Сәйкестендіру негіздері) терминологиялық дау-дамайларды болдырмау үшін қолданылады.

3.22 Кері шақыру сертификаты (revocation certificate): Куәландырылған орталықпен шығарылған және белгілі қауіпсіздік сертификатын кері шақыру туралы хабарлайтын қауіпсіздік сертификаты.

3.23 Кері шақыру тізімінің сертификаты (revocation list certificate): Кері шақырылған қауіпсіздік сертификаттарының тізімі көрсетілген қауіпсіздік сертификаты.

3.24 Симметриялық криптографиялық алгоритм (symmetric cryptographic algorithm): Шифрлеуге және шифрді ашуға бір кілт қолданылатын шифрлеу және тиісті шифрді ашу алгоритмі.

3.25 Куәландырушы орталық (certification authority): Қауіпсіздікпен байланысты деректердің бір немесе бірнеше сыныптарын құрайтын қауіпсіздік сертификаттарын құру (қауіпсіздік саясатының контекстінде) сеніп тапсырылған мән.

3.26 Қауіпсіздік жөніндегі уәкіл (security authority): Қауіпсіздік саясатын анықтауға, іске асырылуына немесе іске қосуына жауап беретін мән.

3.27 Қауіпсіздік домені жөніндегі уәкіл (security domain authority): Қауіпсіздік доменінде қауіпсіздік саясатын іске асыруға жауап беретін қауіпсіздік жөніндегі уәкіл.

3.28 Шартты сенімді мән (conditionally trusted entity): Анықталмай қауіпсіздік саясатын бұза алмайтын қауіпсіздік саясатының контекстіндегі сенімді мән.

3.29 Хэш-функция (hash function): Мәндердің ең төменгі ауқымында жоғары мәндерді (өте үлкен) көрсететін функция (математикалық).

3.30 Қауіпсіздік сертификаттарының тізбекшесі (security certificate chain): Бірінші сертификат қауіпсіздікпен байланысты ақпаратты, ал келесі сертификат – алдыңғы сертификаттардың верификациясы кезінде қолданылуы мүмкін ҚА қамтитын қауіпсіздік сертификаттарының қысқартылған кезектілігі.

3.31 Сандық таңба (digital fingerprint): Криптографиялық бақылау мәні сияқты немесе сипаттамалары бірдей басқа деректер элементін анықтауға жол бермес үшін деректер элементіне мамандандырылған деректерге арналған бір тараптық хэш-функцияларды есептеу нәтижесі сияқты деректер элементінің сипаттамасы.

4 Қысқартулар

Осы стандартта мынадай қысқартулар қолданылады.

4.1 Кіруді басқаратын ақпарат; ҚБА

4.2 Ашық жүйелердің өзара байланысы; АЖӨБ

4.3 Ашық таралған өңдеу; АТӨ

4.4 Қауіпсіздік ақпараты; ҚА

4.5 Сенімді үшінші тарап; СҮТ

5 Белгілеулер

Деңгейлердің қолданылатын белгілеулері [1] анықталған белгілеулерге сәйкес келеді.

Егер өзгелей айтылмаса, сервис термині қауіпсіздік сервисін белгілеуге қолданылады.

Егер өзгелей айтылмаса, сертификат термині қауіпсіздік сертификатын белгілеуге қолданылады.

6 Стандарттың құрылымы

Қауіпсіздік негіздері осы стандарттың құрама бөліктері болып табылады және олар төменде сипатталады. Келешекте Қауіпсіздік негіздерінің қарастырылатын жинағы кеңейтілуі мүмкін. Кілттерді басқару

негіздері осы стандарттың бөлігіне кірмейді, бірақ қолданылу саласы бірдей және олардың сипаттамасы мазмұнды толықтыру мақсатында енгізілген.

6.1 1-бөлім. Шолу

1-бөлімді қараңыз.

6.2 2-бөлім. Сәйкестендіру

Бұл Негіздер ашық жүйелерге қолданылатын сәйкестендірудің барлық аспектілерін, сәйкестендірудің кіруге басқару сияқты қауіпсіздікті қамтамасыз ететін басқа функциялармен байланысын, сонымен қатар сәйкестендіруді басқаруға қойылатын талаптарды сипаттайды.

Осы Негіздер:

a) сәйкестендірудің негізгі түсініктерін;

b) сәйкестендіру механизмдерінің мүмкін кластарды;

c) сәйкестендіру механизмдерінің осы кластарға арналған сервистерді;

d) сәйкестендіру механизмдерінің осы сыныптарын қамтамасыз ететін хаттамаларға қойылатын атқарымдық талаптарды;

e) сәйкестендіруді басқаруға қойылатын жалпы талаптарды анықтайды.

Сәйкестендіру негіздері сәйкестендіру әдістерінің түсінігін, тізбесін және сыныптамасын құрайтын сәйкестендіру стандарттарының жоғарғы иерархиясын қарастырады. Төменде осы әдістердің нақты жинағын егжей-тегжейлі сипаттайтын *ҚР СТ ИСО/МЭК 9798* (*сәйкестендіру тетіктері*) сияқты стандарттар ұсынылған. Ал, иерархияның ең төменгі деңгейіндегі ИСО/МЭК 9594-8 (Сәйкестендіру негіздері) сияқты стандарт нақты қосымшаның немесе талаптардың контекстіндегі әдістерді және түсініктерді қолданады.

Сәйкестендіру негіздері сәйкестендіру моделін, сәйкестендіру бойынша әрекеттерге бөлінетін бірқатар сатыларды, сәйкестендіру ақпараттарымен алмасу үшін сәйкестендіру сертификаттарын қолдануды, осы сатыларға негізделген сәйкестендірудің жан-жақты сервистерін, сонымен қатар сәйкестендірудің жан-жақты сервистерін ұсынатын сәйкестендіру механизмдерінің бес сыныбын қарастырады. Олардың санына сәйкестендіру ақпараттарының ашылуын , сонымен қатар сол (және/немесе басқа) верификаторлардың ашылуын және қайта қолданылуын болдырмайтын механизмдер кіреді.

6.3 3-бөлім. Кіруді басқару

Бұл Негіздер ашық жүйедегі кіруді басқаратын барлық аспектілерді (мысалы, процестерге кіруді, пайдаланушының деректерге, процестің

процеске, процестің деректерге кіруін), сәйкестендіру және аудит сияқты басқа қауіпсіздік сервистерімен өзара байланысты, сондай-ақ, кіруді бақылау үшін басқару талаптарын қарастырады.

Бұл Негіздер:

а) кіруді басқарудың негізгі түсініктерін анықтайды;

б) кіруді басқару бойынша негізгі түсініктер кіруді басқарудың кейбір жалпымен қабылданған сервистерін және механизмдерін қамтамасыз ету үшін қалай нақтыланатындығын көрсетеді;

в) осы сервистерді және кіруді басқарудың тиісті механизмдерін анықтайды;

г) осы сервистерді және кіруді басқарудың тиісті механизмдерін қамтамасыз ететін хаттамаларға қойылатын функционалдық талаптарды анықтайды;

д) осы сервистерді және кіруді басқарудың тиісті механизмдерін қамтамасыз ету үшін басқару талаптарын анықтайды.

е) Кіруді басқару сервистері мен механизмдерінің басқа қауіпсіздік сервистері мен механизмдерімен өзара байланысына қызмет көрсетеді.

Бұл Қауіпсіздік негіздері кіруді басқару үлгісін, кіруді басқару бойынша әрекеттерді бөлетін бірқатар сатыларды, осы сатыларға негізделген кіруді басқаратын жан-жақты сервисті және кіруді басқаратын жан жақты сервисті ұсынатын кіруді басқаратын механизмдердің кем дегенде, үш класын сипаттайды.

6.4 4-бөлім. Істен шықпау

Осы Негіздер осы сервистерді әзірлеу және ұсыну үшін негіздерді құра отырып, ГОСТ ИСО 7498-2:2002 сипатталған істен шықпау сервистерінің тұжырымын нақтылайды және кеңейтеді.

Осы Негіздер:

а) істен шықпаудың негізгі түсініктерін анықтайды;

б) істен шықпаудың жалпы сервистерін анықтайды;

в) істен шықпау сервистерін ұсыну үшін мүмкін механизмдерді идентификациялайды;

г) істен шықпау механизмдері мен сервистері үшін басқару талаптарын сәйкестендіреді.

6.5 5-бөлім. Құпиялық

Құпиялылық сервистің тағайындау ақпараттың рұқсатсыз ашылуынан қорғау болып табылады. Бұл Негіздер таңдау, тарату және басқару кезінде ақпараттың құпиялылығын қамтамасыз етуге арналған.

Осы Негіздер:

а) Негізгі түсініктерді анықтайды;

б) құпиялылық механизмдерінің мүмкін класстарын сәйкестендіреді;

в) құпиялылық механизмдерінің әрбір класының мүмкіндіктерін анықтайды;

г) құпиялылық механизмдерінің класстарын қолдауға қажетті басқару мүмкіндіктерін сәйкестендіреді;

д) құпиялылық механизмдерінің және қосымша сервистердің басқа қауіпсіздік сервистермен және механизмдермен өзара байланысына қызмет көрсетеді.

Осы Қауіпсіздік негіздерінде сипатталған кейбір процедуралар криптографиялық әдістердің көмегімен құпиялықты қамтамасыз етеді. Осы Негіздерді қолдану нақты криптографиялық немесе өзге алгоритмдерді пайдалануға байланысты емес, дегенмен құпиялық механизмдерінің кейбір сыныптары нақты алгоритмнің қасиетіне байланысты болуы мүмкін.

6.6 6-бөлім. Тұтастық

Деректер рұқсатсыз өзгертілмеген немесе бұзылмаған жағдайларды құрайтын қасиет тұтастық деп аталады. Осы Негіздер ақпаратты таңдауда және таратуда және оны басқаруда деректердің тұтастығын қамтамасыз етуге арналған.

Бұл Негіздер:

а) тұтастықтың негізгі түсініктерін анықтайды;

б) тұтастық механизмдерінің мүмкін класстарын сәйкестендіреді;

в) тұтастық механизмдерінің әрбір класының мүмкіндіктерін анықтайды;

г) тұтастық механизмдерінің класын қолдауға қажетті басқару мүмкіндіктерін сәйкестендіреді;

д) тұтастық механизмдерінің және қосымша сервистердің басқа қауіпсіздік сервистермен және механизмдермен өзара байланысына қызмет көрсетеді.

Осы Қауіпсіздік негіздерінде сипатталған кейбір процедуралар криптографиялық әдістердің көмегімен тұтастықты қамтамасыз етеді. Осы Негіздерді қолдану нақты криптографиялық немесе өзге алгоритмдерді пайдалануға байланысты емес, дегенмен құпиялық механизмдерінің кейбір сыныптары нақты алгоритмнің қасиетіне байланысты болуы мүмкін.

Осы Негіздердің контекстіндегі ақпараттың тұрақтылығы емес, деректердің тұрақты мәндері сияқты тұтастығы осы деректермен ұсынылған. Басқаша өзгеру түрлері болмайды.

6.7 7-бөлім. Қауіпсіздік аудиті және дабыл белгісі

Бұл Негіздер:

а) қауіпсіздік аудитінің және дабыл сигналының негізгі түсініктерін анықтайды;

б) қауіпсіздік аудитінің және дабыл сигналының жалпы моделін ұсынады;

в) қауіпсіздік аудитінің және дабыл сигналының басқа қауіпсіздік сервистерімен өзара байланысын сәйкестендіреді.

Басқа қауіпсіздік сервистері сияқты, қауіпсіздік аудитты қауіпсіздік саясатының анықталған контекстінде ғана қамтамасыз етілуі мүмкін. Қауіпсіздік саясаты қауіпсіздік жөніндегі уәкілдермен олардың қауіпсіздік домендері шегінде анықталады. Осы Негіздерге базаланатын механизмдерді өзгешелендіретін кез келген стандарт әртүрлі қауіпсіздік саясатын қолдай білу керек.

6.8 Кілттерді басқару

Кілттерді басқару бойынша негізгі ережелер (ҚР СТ ИСО/МЭК 11770 стандартының 1-бөлімі) қалған Қауіпсіздік негіздерімен ерекше байланысқа ие, себебі ол *МСТ ИСО 7498-2:2002* анықталған қауіпсіздік сервистерімен тікелей байланысты емес қызметтерді қарастырады. Бұл қызметтер шифрлеу немесе сандық қолтаңба қолданылатын ақпараттық технологиялардың кез келген ортасында қолданылады.

Бұл Негіздер:

а) кілттерді басқару мақсаттарын сәйкестендіреді;

б) кілттерді басқаратын тетіктер негізіндегі жалпы модельдерді сипаттайды;

в) кілттерді басқару бойынша негізгі түсініктерді, осы стандарттың барлық құрама бөліктері үшін жалпы түсініктерді анықтайды;

г) кілттерді басқаратын сервистерді анықтайды;

д) кілттерді басқаратын механизмдердің сипаттамаларын сәйкестендіреді;

е) кілт материалдарын оның қолданылу мерзімінде басқаруға қойылатын талаптарды өзгешелендіреді;

ж) кілт материалдарын оның қолданылу мерзімінде басқару бойынша негізгі ережелерін сипаттайды.

7 Жалпы түсініктер

Көптеген түсініктер Қауіпсіздік негіздерінің бірнеше бөлімдеріне талап етіледі. Стандарттың осы бөлімі осы түсініктерді осы стандарттың басқа бөліктерінде кезекті қолданылу үшін анықтайды.

7.1 Қауіпсіздік ақпараты

Қауіпсіздік ақпараты (ҚА) – бұл қауіпсіздік сервистерін іске асыруға қажетті ақпарат. ҚАың мысалдары болып табылады:

– қауіпсіздік саясатының ережелері;

– сәйкестендіру ақпараты (АА) және кіруді басқару ақпараты (КБА) сияқты нақты қауіпсіздік сервистерін іске асыруға арналған ақпарат;

– қауіпсіздік белгілері, криптографиялық бақылау мәндері, қауіпсіздік сертификаттары және қауіпсіздік маркерлері сияқты қауіпсіздік механизмдеріне қатысты ақпарат.

ҚП түрлері, Қауіпсіздік бірнеше негіздер үшін жалпы түсініктер 8-тарауда қарастырылады.

7.2 Қауіпсіздік домені

Қауіпсіздік домені қауіпсіздік әрекеттермен нақты байланысты топтар үшін қауіпсіздік жөніндегі бір уәкілмен басқарылатын қауіпсіздіктің берілген саясатына бағынатын элементтер жинағын қарастырады. Қауіпсіздік доменіндегі әрекеттер осы қауіпсіздік доменінің бір немесе бірнеше элементтерімен жүргізіледі және басқа қауіпсіздік домен элементтерімен жүргізілуі де мүмкін.

– Элементтерге қол жеткізу;

– ВОС (N)-деңгей қосылысын белгілеу немесе пайдалану;

– нақты басқару функциясымен байланысты операциялар;

– нотариатты қамтитын істен шықпау операциялары әрекеттер үлгісі болып табылады.

Әрекет қауіпсіздікпен байланысты болуы мүмкін, тіпті егер ол қазіргі уақытта оны пайдалану бойынша өзіндік саясатты қолдануға енгізетін механизмдердің субъектілері болып саналмайды және келешекте басқару механизмдерінің субъектілері болуы мүмкін.

Ашық жүйелер ортасындағы қауіпсіздік домені элементтерінің мысалдары нақты ашық жүйелер, қолданбалы процестер, (N)-мәндер, (N)-деректердің хаттамалық блоктары, қайта таратқыштар және нақты ашық жүйелерді пайдаланушы-адамдар сияқты логикалық немесе физикалық элементтер болып табылады. Кейде пайдаланушы-адамдарды қауіпсіздік доменінің басқа элементтерінен айыра білу керек. Мұндай жағдайларда адамдар болып саналмайтын объектілерді белгілеу үшін «деректер объектілері» термині қолданылуы мүмкін.

7.2.1 Қауіпсіздік саясаты және қауіпсіздік саясатының ережелері

Қауіпсіздік ережесі жалпы түрдегі қауіпсіздік домені үшін қауіпсіздік талаптарын білдіреді. Мысалы, қауіпсіздік саясаты белгілі жағдайларда жұмыс істеуде қауіпсіздік доменінің барлық мүшелері немесе қауіпсіздік доменіндегі барлық ақпараттар үшін талаптарды анықтау қажет. Қауіпсіздік саясатын іске асыру оны қанағаттандыратын қауіпсіздік сервистерін сәйкестендіруге жеткізеді. Іске асыру үшін қауіпсіздік механизмдері таңдап алынады. Қауіпсіздік механизмдерін таңдау туралы шешім болжамды қауіп-

қатерлерден және қорғалатын ресурстардың құндылығына байланысты болады.

Қауіпсіздік саясаты жалпы қағидаттар түрінде табиғи тілде формуланады. Бұл қағидаттар қауіпсіздік доменінің нақты ұйым немесе оның мүшелері үшін қауіпсіздік талаптарын белгілейді. Осы қауіпсіздік талаптары нақты жүйеде белгіленгенге дейін, қауіпсіздік саясаты одан қауіпсіздік саясатының ережелер топтамасын алуға болатындай нақтылануы тиіс. Осы талаптарды қауіпсіздік саясатының ережелері түрінде түсіндермесі техникалық әрекет болып табылады. Қауіпсіздік саясаты белгілі әрекеттердің орындалуын талап еті немесе орындалуына тыйым салып оның субъектілері болып табылатын элементтер әрекетін шектейді. Қауіпсіздік саясаты элементтерге белгілі әрекеттерге қатысуына рұқсат бере алады. Мұндай қауіпсіздік саясатының түсіндірмесі АШӨ қаралатын *ГОСТ ИСО 7498-2* салыстырғанда кеңірек сипатталады. Нақты қауіпсіздік сервисіне тән қауіпсіздік саясатының аспектілері осы сервиске арналған Қауіпсіздік негіздерін қарастырғанда талқыланады.

Қауіпсіздік доменіне арналған қауіпсіздік саясатының екі түрлі ережелері бар: модемішілік және домен арасындағы әрекеттер. Екінші қауіпсіздік саясатының ережелері қауіпсіз өзара байланысу ережелері деп аталады. Сондай-ақ, қауіпсіздік саясаты байланыс үшін барлығымен бірге, ал нақты қауіпсіздік домендерімен қандай ережелер қолданылатындығы жайында анықтай алады.

Жүйе немесе әрекеттер модификациясы және қауіпсіздік домені үшін қауіпсіздік саясаты өзгергенде қауіпсіздік домені үшін қауіпсіздік саясаты ережелерінің өзектілігі қамтамасыз етілуге тиіс.

Ескертпе – Бұл Негіздер қауіпсіздік саясатының мына аспектілеріне қолданылмайды:

- қауіпсіздік саясатын дербес немесе қамтамасыз ететін тарап;
- қауіпсіздік саясатын белгілейтін немесе қамтамасыз ететін процедуралар;
- қауіпсіздік саясатының мазмұны;
- қауіпсіздік доменіне қауіпсіздік саясатын байланыстыру процедуралары.

7.2.2 Қауіпсіздік домені жөніндегі уәкіл

Қауіпсіздік домені жөніндегі уәкіл — бұл қауіпсіздік домені үшін қауіпсіздік саясатының іске асырылуына жауап беретін қауіпсіздік жөніндегі уәкіл.

Қауіпсіздік домені жөніндегі уәкіл:

құрама мәні болуы мүмкін, мұндай мән сәйкестендірілуге тиіс;

қауіпсіздік домені жөніндегі уәкіл субъекті болып табылатын қауіпсіздік саясатына байланысты бір немесе бірнеше мәндерге қауіпсіздік саясатының іске асырылу жауапкершілігін жүктеуі мүмкін;

- қауіпсіздік доменінің элементтеріне қатысты өкілеттіктерді иемденеді.

Ескертпе – Егер қауіпсіздік домені жөніндегі уәкіл ешқандай шектеу қоймайтын болса, қауіпсіздік саясаты бос болуы мүмкін.

Екі қауіпсіздік домені жөніндегі уәкілдер, егер өздерінің қауіпсіздік саясаттарын үйлестіре алатын болса, бір-бірімен байланысты болады дейді.

7.2.3 Қауіпсіздік домендері арасындағы өзара байланыс

Қауіпсіздік доменінің түсінігі мына екі себеп бойынша маңызды ұсынылады:

– қауіпсіздік қалай басқарылатындығы және жүргізілетіндігі сипатталу үшін ол қолданылуы мүмкін;

– қауіпсіздікпен байланысты әрекеттерді модельдеу және қауіпсіздік жөніндегі әртүрлі уәкіл басқаратын элементтерді қамтитын ол құрылыс блогы ретінде қолданылуы мүмкін.

Қауіпсіздік домендері бір немесе бірнеше тәсілдермен байланысты болуы мүмкін. Мұнда қауіпсіздік домендерінің кейбір өзара байланысу мүмкіндіктері талқыланады. Қауіпсіздік домендері арасындағы өзара байланыс қауіпсіздік домендерінің қауіпсіздік саясатында қауіпсіздік жөніндегі уәкілмен келісілген түрінде белгіленуі мүмкін. Бұл өзара байланыстар қауіпсіздік домендерінің элементтері және әрекеттері терминдерінде қарастырылады және өзара байланысты әрбір қауіпсіздік домендеріне арналған қауіпсіз өзара байланысу ережелерінде белгіленеді. Қауіпсіздік домендерінің кейбір нақты өзара байланыстары осы тараудың келесі бөлімдерінде сипатталады. Қауіпсіздік домендерінің көптеген басқа өзара байланыстары болуы мүмкін.

а) Егер екі қауіпсіздік доменінде деректердің жалпы объектілері және жалпы әрекеттері болмаса және сәйкесінше, олар өзара байланыса алмаса, олар **оқшауланған** болып табылады.

б) Екі қауіпсіздік домені, егер:

– оларда деректердің жалпы объектілері болмаса;

– әрбір қауіпсіздік доменінің ішіндегі әрекеттер олардың жеке қауіпсіздік саясаттарына ғана бағынатын болса (және тиісті түрде қауіпсіздік саясатының ережелер топтамасы болса);

– қауіпсіздік домендері жөніндегі уәкілдер олардың қауіпсіздік саясаттарын үйлестіруге міндетті болмаса олар бір-бірінен **тәуелсіз** деп аталады.

Екі немесе бірнеше тәуелсіз қауіпсіздік домендері ақпаратты бірігіп қолдануды үйлестіру туралы келісім жасау шешімін қабылдай алады (7.2.4 тарауын қараңыз).

в) Егер:

– А көптеген элементтер В элементтерінің көп болса немесе олармен сәйкес болса;

– А көптеген әрекеттер В көптеген әрекеттері болып табылса немесе олармен сәйкес болса;

– А юрисдикциясын А қауіпсіздік жөніндегі уәкілдің В қауіпсіздік жөніндегі уәкілге жүктейтін болса;

– А қауіпсіздік саясаты В қауіпсіздік саясатына қайшы келмесе. Егер қажет болса және В қауіпсіздік саясаты рұқсат берсе, А қосымша қауіпсіздік саясатын ендіре алатын болса А қауіпсіздік домені В басқа қауіпсіздік доменінің **қауіпсіздік доменіне бағынатын домен** деп аталады .

1 Ескертпе – Көптеген қатарына бірнеше есе көп ұғымы сәйкес болуы мүмкін. Соңғы шектерге байланысты, қауіпсіздік доменіне бағынатын домен әрекеттердің кейбір сыныптары үшін қауіпсіздік доменінің көптеген элементтерінен және басқа шектерге байланысты — қауіпсіздік доменінің көптеген элементтерінің бірнеше есе көп элементтерінің барлық әрекеттерінің сыныптарынан құрастырылуы мүмкін. Осы екі шектерге байланысты көптеген аралық нұсқалар болуы мүмкін.

г) А қауіпсіздік домені В А қауіпсіздік доменіне бағынған жағдайда В **басқа доменнің қауіпсіздік домені** деп аталады.

2 Ескертпе – Осы Қауіпсіздік негіздері оқшауланған, тәуелсіз, доменге бағыну және доменге бағынбау түсініктері қандай да бір нақты хаттамалармен, өзгешеліктермен немесе іске асырулармен қамтамасыз етілу үшін талап етілмейді.

7.2.4 Қауіпсіз өзара байланысу ережелерін белгілеу

Қауіпсіздік домендері арасындағы ақпараттық алмасу мүмкін болды, ол алмасу үшін қауіпсіз өзара байланысу ережелері деп аталатын қауіпсіздік саясаты ережелерінің келісілген топтамасы болады. Әрбір қауіпсіздік домені үшін олар қауіпсіздік саясаты ережелерінің бөлігі болып табылады. Қауіпсіз өзара байланысу ережелері келіссөздер арқылы қауіпсіздіктің жалпы сервистері мен механизмдерін және өзара байланысты қауіпсіздік домендерінің әрқайсысындағы қауіпсіздік ақпараттарының қауымдасқан элементтерін белгілеу арқылы таңдауға мүмкіндік береді. Қауіпсіздік домендері қауіпсіз өзара байланысу ережелерін қолдауға қажетті қауіпсіздікті басқаратын ақпаратпен алмасуы мүмкін. Қауіпсіздік домендері арасындағы өзара әрекеттесуге байланысты қауіпсіз өзара байланысу ережелері әртүрлі тәсілдермен анықталуы мүмкін.

Тәуелсіз қауіпсіздік домені арасындағы қауіпсіз өзара байланысу үшін қауіпсіз өзара байланысу ережелері өзара байланысатын қауіпсіз домендер жөніндегі уәкілмен келісілуге тиіс.

Қауіпсіздік домендерінің тармақтары арасындағы қауіпсіз өзара байланысу үшін қауіпсіз өзара байланысу ережелері қауіпсіздік домендерін басқаратын уәкілмен белгіленуі мүмкін. Егер қауіпсіздік доменін басқарушы қауіпсіздік саясаты мүмкіндік берсе, қауіпсіздік доменінің тармақтары өздерінің қауіпсіз өзара байланысу ережелерін белгілей алады.

7.2.5 Домендер арасында қауіпсіздік ақпараттарын тарату

Қауіпсіз өзара байланысу ережелері өздері қауіпсіздік ақпараттарын бере алады және қауіпсіздік домендер арасында осы ақпараттың таратылуы талап етілуі мүмкін. Мына жағдайлар қарастырылады:

– барлық қауіпсіздік домендерінде ақпараттың семантикасы және ұсынылуы ұқсас. Яғни, тарату талап етілмейді.

– ҚАың семантикасы барлық қауіпсіздік домендерінде ұқсас, бірақ олардың ұсынылуы ерекшеленеді. Бұл қауіпсіздік ақпараттарын сипаттау тәсілдері әртүрлі екендігін білдіреді, сондықтан синтаксикалық тарату талап етіледі.

– Қауіпсіздік ақпараттың семантикасы және ұсынылуы барлық қауіпсіздік домендерінде әртүрлі. Бұл қауіпсіз өзара байланысу ережелері бір доменнің қауіпсіздік ақпараттары басқа доменнің қауіпсіздік ақпараттарына қалай таратылатыны анықталуы тиіс. Сондай-ақ, синтаксикалық тарату талап етілуі мүмкін.

7.3 Қауіпсіздіктің нақты сервистері үшін қауіпсіздік саясаттарын қарастыру

Тұтастық сервисін немесе құпиялық сервисін кейбір іске асыру кезінде кіруді басқару механизмдері қолданылуы мүмкін. Мұндай жағдайларда Тұтастық сервисін немесе құпиялық сервисін іске асыруға қатысты қауіпсіздік саясатының ережелері кіруді басқару механизмдері қалай қолданылатындығын сипаттау керек. Кіруді басқару механизмдері инициаторлардың терминдерінде және мақсаттарында сипатталады (ҚР СТ ИСО/МЭК 10181-3). Қауіпсіздік саясатының ережелері инициаторлармен және мақсаттарымен кіруді басқару механизмдерінде тұтастық және құпиялылық саясатының мәндері, ақпараттары және элементтері қалай байланысты болатындығын анықтайды.

Құпиялылық саясаттары мәндер ақпарат элементтерін сұрай алатын терминдерде формаланады. Бастамашымен орындалатын мәндер үшін ақпаратты аша алатын әрекеттер бойынша екі жолы бар. Біріншіден, әрекет ету нәтижесі бастамашыға мақсаттары туралы кейбір ақпарат бере алады. Екіншіден, әрекет ету сұранысы бастамашы туралы кейбір ақпараттың мақсаттарын бере алады. Кіруді басқару механизмдері құпиялық сервистерін ұсынуға қолданылатын болса, ақпарат алуға тырысатын мән бастамашы, ал ақпарат элементтері мақсаттар болып саналады.

Тұтастық саясаттары мәндер деректердің элементтерін өзгерте алатын терминдерде формаланады. Бастамашымен орындалатын мәндер үшін ақпаратты аша алатын әрекеттер бойынша екі жолы бар. Біріншіден, әрекет ету нәтижесі бастамашыға мақсаттары туралы кейбір ақпарат бере алады. Екіншіден, әрекет ету сұранысы бастамашы туралы кейбір ақпараттың

мақсаттарын бере алады. Кіруді басқару механизмдері құпиялық сервистерін ұсынуға қолданылатын болса, ақпарат алуға тырысатын мән бастамашы, ал ақпарат элементтері мақсаттар болып саналады.

7.4 Сенімді мәндер

Егер мән қауіпсіздік саясатын бұза алатын болса немесе ол күтпеген әрекеттерді орындамаса немесе күтілетін әрекеттерді сәтсіз орындайтын болса, мән қауіпсіздік саясатының қосымша мәтіндегі әрекеттердің кейбір сыныптары үшін **сенімді мән** деп аталады Қауіпсіздік саясаты қандай мәндер сенімді екендігін анықтайды және әрбір сенімді мән үшін сенімді болып табылатын әрекеттер топтамасын анықтайды. Кейбір әрекеттер жинағы үшін сенімді болып табылатын мән қауіпсіздік домені ішінде барлық әрекеттерге сенімді болуы міндетті емес.

Мән белгілі түрде жүргізілетіндігін қауіпсіздік саясатында декларациялау мәннің тиісті жүргізілуіне кепілдік бермейді. Сәйкесінше, қауіпсіздік саясаты сенімді мәннің әрекетсіздігінен туындаған қауіпсіздік саясатының бұзылыстарын анықтау құралдарын талап етуі мүмкін. Әрекетсіздігі анықталмайтын сенімді мән **сөзсіз сенімді мән** деп аталады. Қауіпсіздік саясатын бұзатын, бірақ анықталмай қалмайтын сенімді мән *шартты сенімді мән* деп аталады.

Сенімді мән өзінің көптеген әрекеттері үшін сөзсіз сенімді, және – өзінің көптеген басқа әрекеттері үшін шартты сенімді болуы мүмкін. Мұндай мән қауіпсіздік саясатының кейбір аспектілерін бұзуы мүмкін, бірақ анықталмай қауіпсіздік саясаттарының басқа аспектілерін бұза алмайды.

Қауіпсіздік доменінің қауіпсіздік саясаты қауіпсіздік доменіне кірмейтін элемент қауіпсіздік доменінің ішінде кейбір көптеген әрекеттер үшін сенімді болып табылатындығы жайында декларация жасай алады. Қауіпсіз өзара байланысу ережелері (7.2.4 тармағын қараңыз) қауіпсіздік доменінің ішкі мәндері қауіпсіздік домені үшін сыртқы сенімді мәнмен өзара байланысу керектігін анықтай алады.

7.5. Сенім

X мәні кейбір әрекеттер жинағы шегінде және X мәні осы шектерде Y мәнінің тиісті әрекетіне сүйенген жағдайда Y мәніне сенеді дейді.

Сенім өзара байланыста болмауы мүмкін. Сенімді мән болып саналмайтын мін сенімді мәнмен ұсынылатын сервистерді қолдануы мүмкін. Сенімнің өзара байланысты болу мысалы екі сенімді мәндер әрекеттерді орындау кезінде бірігетін жағдайлар болып табылады, және олардың әрқайсысы қауіпсіздік саясатының өмірінде басқаның көмегіне жүгінеді.

Сенім транзитивтік болуы міндетті емес. Нақты жағдайларда қауіпсіздік саясаты сенімнің транзиттілігін анықтай алады. Егер А мәні В сенімді мәнмен ұсынылатын сервистерге жүгінетін болса, ал В сенімді мән

С сенімді мәнмен ұсынылатын сервистерге жүгінетін болса, онда А С сенімді мәнге жүгінетін болады. Егер бұл расында осылай болса, сенім транзиттік болып саналады. Бірақ, басқа жағдайларда В С әрекетсіздігі А әрекетіне әсер етпейтіндігіне кепілдік беретін шараларды қабылдайды. Бұл жағдайда сенім транзиттік болмайды.

7.6 Сенімді үшінші тараптар

Сенімді үшінші тарап – бұл қауіпсіздік жөніндегі уәкіл немесе қауіпсіздік әрекеттеріне қатысты сенімді (қауіпсіздік саясатының контекстінде) болып табылатын оның агенті.

Сенімді үшінші тараптардың үлгілері:

– сәйкестендіру кезіндегі сенімді үшінші тарап;

– істен шықпау үшін уақытша мөртабан қоятын нотариат немесе сервис;

– кілттерді басқару кезінде кілттерді тарату орталығы.

8 Қауіпсіздіктің әмбебап ақпараты

Қауіпсіздік ақпаратының кейбір түрлері бірнеше Қауіпсіздік негіздерінің сипаттамасын талап етеді. Осы тарауда қауіпсіздік ақпаратының осы түрлері сипатталады.

Қауіпсіздік негіздерінде сипатталған қауіпсіздік механизмдері, әдетте, өзара байланысу үшін қауіпсіздік сервистері қажет мәндер арасында немесе қауіпсіздік және өзара байланысу мәндері жөніндегі уәкіл арасында қауіпсіздік ақпараттарымен алмасуды қамтиды. Осы Негіздерде сипатталатын механизмдермен қауіпсіздік ақпаратының төрт жалпы түрлері:

– байланыс элементіне, арнасына немесе деректер бірлігіне қолданылатын қауіпсіздік саясатының нұсқаулары үшін қолданылатын қауіпсіздік белгілері;

– деректер бірлігінің өзгерістерін анықтауға қолданылатын криптографиялық бақылаулы мәні;

– қауіпсіздік жөніндегі уәкілмен немесе бір немесе бірнеше өзара байланысты тараптармен қолдану үшін ДТС алынған қауіпсіздік ақпараттарын қорғауға қолданылатын қауіпсіздік сертификаттары;

– өзара байланысты тараптар арасында таратылатын қауіпсіздік ақпараттарын қорғауға қолданылатын қауіпсіздік маркерлері қолданылады.

Ескертпе – Қауіпсіздік ақпараты бірнеше әртүрлі қауіпсіздік механизмдерімен қорғалуы мүмкін. Кейбір қауіпсіздік механизмдері криптографияның қолданылуына негізделеді, басқалары физикалық құралдарды қолданады.

8.1 Қауіпсіздік белгілері

Қауіпсіздік белгісі – бұл байланыс элементтерімен, арналарымен немесе деректер бірлігімен байланысты қауіпсіздік атрибуттарының жинағы. Сондай-ақ, қауіпсіздік белгісі белгіні қолдану үшін пайдаланылатын байланыстыруды және қауіпсіздік саясатын құруға жауап беретін қауіпсіздік жөніндегі уәкілді көрсетеді. Қауіпсіздік белгісі қауіпсіздік сервистерінің үйлесімін қамтамасыз ету үшін қолданылады.

Қауіпсіздік белгілерін пайдалану мысалдары ретінде:

– тұтастықты және/немесе құпиялықты қамтамасыз ету үшін кіруді басқаруды қамтитын кіруді басқару сұлбасының қауіпсіздік белгісіне негізделген қамтамасыз ету;

– оларды өңдеу бойынша деректер және талаптар болып табылатын сенім дәрежесінің нұсқауы;

– оларды өңдеу бойынша деректер және талаптар болып табылатын сезімталдық нұсқауы;

– қорғау, орналастыру бойынша талаптардың және жүгіну бойынша басқа талаптардың нұсқауы қызмет атқарады.

8.2 Криптографиялық бақылау мәні

Криптографиялық бақылау мәні — бұл деректер блогын криптографиялық түрлендіру арқылы шығарылатын ақпарат. Үш криптографиялық бақылау мәндері пломбалар, сандық қолтаңбалар және сандық таңбалар.

Пломба симметриялық криптографиялық алгоритм және бір-бірімен байланысатын мәндерге арналған құпиялы кілт көмегімен есептелетін криптографиялық бақылау мәнін білдіреді. Пломбалар тарату барысында деректердің өзгеруін анықтау үшін қолданылады.

Сандық қолтаңба – бұл алушымен жасандыдан қорғайтын және жабық кілт және асимметриялық криптографиялық алгоритм көмегімен есептелетін криптографиялық бақылау мәні. Сандық қолтаңбаны тексеру осы криптографиялық алгоритмнің Сандық қолтаңбаны тексеру осы криптографиялық алгоритмді және тиісті ашық кілтті қолдануды талап етеді.

Ескертпелер

1. Дегенмен алушыға криптографиялық бақылау мәнін жасанды түрде жасауға мүмкіндік бермейтін басқа да құралдар кездеседі (мысалы, олардың жұмысына араласуға берік криптографиялық модульдерді қолдану), Қауіпсіздік негіздерінде «сандық қолтаңба» ассиметриялық криптографиялық алгоритм арқылы алынған криптографиялық бақылау мәндерін белгілеуге қолданылады.

2. Кейбір асимметриялық криптографиялық алгоритмдерде сандық қолтаңбаны есептеу бірнеше жабық кілттердің қолданылуын талап етеді. Осыған ұқсас алгоритмдерді қолданған жағдайда жабық кілттерді пайдалану әртүрлі мәндермен ғана мүмкін болады. Бұл мәндер сандық қолтаңбаны құру үшін біріктірілуі тиіс.

Сандық таңба — бұл осындай сандық таңбасымен басқа деректерді анықтауға мүмкін болмау үшін деректерге өзгешелігі жеткілікті деректер элементінің сипаттамасы. Сандық таңба ретінде криптографиялық бақылау мәндерінің кейбір түрлері (мысалы, біртараптық функциялардың деректеріне қолданылатын нәтиже) қолданылуы мүмкін. Сандық таңбалар криптографиялық алгоритмдерден ерекшеленетін басқа тәсілдермен алынуы мүмкін. Мысалы, сандық таңба деректер элементінің көшірмесі болып табылады.

3. Бір тараптық функциялар сандық таңбаларға баламалы емес. Кейбір бір тараптық функциялар сандық таңбаларды құруға сәйкес келмейді, ал кейбір сандық таңбалар бір тараптық функцияларды пайдаланбай құрылады.

4. Асимметриялық алгоритм көмегімен сандық таңбаны есептеу асимметриялық алгоритмдер көптеген есептеуді талап етуіне байланысты көп уақытты қажет етуі мүмкін. Сандық таңба деректердің өзімен емес, деректердің сандық іздері бойынша анықталуы мүмкін. Бұл тиімділікті арттыруы мүмкін, себебі ұзақ хабарламамен салыстырғанда, қысқа сандық таңбаға арналған сандық қолтаңбаны анықтау жылдам орындалады.

Криптографиялық бақылау мәні деректердің бірлік блоктарын іске қосылуынан міндетті түрде қорғамайды. Іске қосылудан қорғау деректерге іске қосылуды анықтауға қолданылатын кейбір ақпараттарды енгізу арқылы қол жеткізуге болады. Мысалы, реттік нөмірді немесе уақытша белгіні немесе криптографиялық тіркемені қолдану. Іске қосылудан қорғауды қамтамасыз ету үшін ақпарат деректердің қорғалған блоктары алушымен тексерілуге тиіс.

8.3. Қауіпсіздік сертификаттары

8.3.1 Қауіпсіздік сертификаттарына кіріспе

Қауіпсіздік сертификаты қауіпсіздік жөніндегі уәкілмен немесе сенімді үшінші тараппен тұтастық және сәйкестендіру сервисінің деректері үшін дерек көздерін қамтамасыз ету кезінде қолданылатын қауіпсіздік ақпаратымен бірге ұсынылған деректердің қауіпсіздігімен байланысты топтамаларды қарастырады. Қауіпсіздік сертификаты деректердің жарамдылық мерзімдерін көрсетеді.

Қауіпсіздік сертификаттары мәндердің қауіпсіздігі жөніндегі уәкілден (немесе сенімді үшінші тараппен) қауіпсіздік ақпаратын тарату үшін қолданылады, бұл ақпарат қауіпсіздік функцияларын орындау үшін талап етіледі. Қауіпсіздік сертификаты бірнеше қауіпсіздік сервистері үшін қауіпсіздік ақпараттарын қамтиды.

Басқа Қауіпсіздік негіздерінде сипатталғандай, қауіпсіздік сертификаты төмендегілер үшін қолданылатын қауіпсіздік ақпараттарын:

– кіруді басқаруды;
– сәйкестендіруін;
– тұтастықты сақтауды;
– құпиялықты сақтауды;

– істен шықпауды;
– аудитті;
– кілттерді басқаруды қамтуы мүмкін.

8.3.2 Қауіпсіздік сертификаттарын верификаттау және тіркеу

Қауіпсіздік сертификатын верификациялау оның тұтастығын тексеру, қауіпсіздік сертификатын шығарған ұсынымды мәннің түпнұсқалығын растау және осы мән қауіпсіздік сертификаттарын шығаруға құқылығын тексеру болып табылады. Бұл операциялар қосымша ҚА ұсынуды талап етеді.

Егер қауіпсіздік сертификатының верификаторында қауіпсіздік сертификатын верификаттау үшін талап етілетін ҚА болмаса, ҚА ұсыну үшін басқа қауіпсіздік жөніндегі уәкілден алынған қауіпсіздік сертификаты қолданылуы мүмкін. Бұл процесс қауіпсіздік сертификаттарының тізбегін алу үшін қайталануы мүмкін. Олар белгілі қауіпсіздік жөніндегі уәкілден сертификатталған қауіпсіздік ақпараты талап етілетін мәнге дейін қауіпсіз маршрутты ұсынатын ҚА жауап береді (яғни, ҚА белгіленген).

Қауіпсіздік сертификаттарының тізбегін барлық қауіпсіздік саясаттарымен жүктелетін шектеулерге сәйкес болған жағдайда қолдану керек. Тізбектің болуы жеткіліксіз. Тізбекті осыған ұқсас пайдалану тізбек верификаторымен және тізбекте сертификаттар құрған қауіпсіздік жөніндегі уәкіл арасындағы, сонымен қатар осы қауіпсіздік жөніндегі уәкілдер арасындағы сеніммен рұқсат етілген жағдайда ғана қолданған дұрыс. Бұл қатынастар сертификаттар тізбегінің верификаторының қауіпсіздік саясатымен және қауіпсіздік жөніндегі уәкілдің қауіпсіздік саясаттары арасында анықталады. Оның ішінде, кейбір қауіпсіздік жөніндегі уәкілдер кейбір басқа қауіпсіздік жөніндегі уәкілдер үшін қауіпсіздік сертификаттарын шығару сеніп тапсырылған, ал кейбір басқаларға олар басқаратын мәндер үшін қауіпсіздік сертификаттарын шығару тапсырылған.

8.3.3 Қауіпсіздік сертификаттарын шақыру

Қауіпсіздік сертификатында мазмұндалатын қауіпсіздік ақпараттары жарамсыз болуы мүмкін. Мысалы, жабық кілтті компрометациялау кезінде тиісті ашық кілт қолданылмау керек және сәйкесінше, осы ашық кілтті қамтитын қауіпсіздік сертификаттары кері шақыртылуы тиіс.

Қауіпсіздік сертификаттарын шақыруға қолданылатын механизмдер шақыру сертификаттарын және шақыру тізімінің сертификаттарын қамтиды. *Шақыру сертификаты* - бұл нақты қауіпсіздік сертификатының шақырылғандығын көрсететін қауіпсіздік сертификаты. *Шақыру тізімінің сертификаты* – бұл шақырылған қауіпсіздік сертификаттарының тізімін сәйкестендіретін қауіпсіздік сертификаты.

8.3.4 Қауіпсіздік сертификаттарын қайтадан қолдану

Кейбір қауіпсіздік сертификаттары көптеген өзара әрекеттерді қолдау мақсатында пайдалануға арналған, ал басқалары бір реттік пайдаланылады. Бірнеше рет пайдаланылатын қауіпсіздік сертификатының мысалы *ИСО/МЭК 9594-8* стандартында анықталған сәйкестендіру сертификаты болып табылады. Бір реттік пайдаланылатын қауіпсіздік сертификатының мысалы бір рет кіруге рұқсат беретін кіруді басқару сертификаты жатады. Бір реттік пайдаланылатын қауіпсіздік сертификаттары олардың қайталап пайдаланылуын болдырмайтын ақпараттарды (мысалы бірегей нөмірі) қамтиды.

8.3.5 Қауіпсіздік сертификатының құрылымы

Қауіпсіздік сертификатының жалпы түрі үш құрама бөлігі:

– барлық қауіпсіздік сертификаттарында талап етілетін ақпарат;

– бір немесе бірнеше қауіпсіздік сертификаттарға сәйкес келетін қауіпсіздік ақпараттары;

– қауіпсіздік ақпараттарының пайдаланылуын бақылайтын немесе шектейтін ақпараттар болады.

Барлық қауіпсіздік сертификаттарында талап етілетін ақпарат екі санатқа бөлінеді:

а) тұтастықты сияқты, дерек көздерін сәйкестендіруді қамтамасыз ететін ақпараттар (мысалы, криптографиялық бақылау мәні және верификаттауға қолданылатын ақпарат көрсеткіштері). Себебі дерек көздерін сәйкестендіру сервисі ұсынылғанда, қауіпсіздік сертификатының жарияланған дерек көздерінің идентификаторын көрсеткіші (яғни уәкілетті органды шығарған) ұсынылуға тиіс.

б) Жарамдылық мерзімі идентификацияланатын (мысалы, анық жарамдылық мерзімі) немесе көрсетілген ақпараттар (мысалы, құрылу уақыты және жарамдылық мерзімі анық емес). Бұл қауіпсіздік сертификатының бірнеше рет шектеусіз қолданылуын болдырмайды, дегенмен қауіпсіздік сертификаты жарамдылық мерзімінде бірнеше рет қолданыла алады.

Қауіпсіздік ақпараттарын бақылайтын немесе шектейтін ақпарат үш санатқа бөлінеді:

а) Қауіпсіздік сертификаттарын рұқсатсыз пайдаланудан қорғайтын ақпараттар.

Мысал ретінде:

– ҚА қауіпсіздік сертификаттарына енген мәнді немесе мәндерді сәйкестендіретін ақпарат (мысалы, ерекше идентификатор);

– қауіпсіздік сертификатында мазмұндалатын ҚА пайдалануға рұқсат етілген мәндерді сәйкестендіретін ақпарат;

– сертификаттың неше рет қолданыла алатынын бақылайтын ақпарат;

– қауіпсіздік сертификаты қолданылатын қауіпсіздік саясатын сәйкестендіретін ақпарат;

– қауіпсіздік сертификаттарын ұрлаудан қорғауға арналған қорғау әдістері және қауымдасқан параметрлер (А қосымшасындағы мысалдарды қараңыз);

– таратылудан қорғауға қолданылатын ақпарат (мысалы, бірегей нөмір немесе сұраныс) қызмет атқарады.

б) Қауіпсіздік аудиті мақсатында қолданылатын ақпараттар.

Мысалға:

– қауіпсіздік жөніндегі уәкілмен немесе агентпен шығарылған барлық қауіпсіздік сертификаттарына қолданылатын қауіпсіздік сертификаты үшін бірегей қауіпсіздік сертификатының сілтемелі идентификаторы (мысалы, реттік нөмір);

– бастапқыда сертификат берілген мәндер идентификаторы (аудит мақсаты үшін) енеді.

в) Қауіпсіздікті қалпына келтіру мақсатында қолданылуы мүмкін ақпараттар.

Оның мысалдары:

– нақты қауіпсіздік сертификатын шақыруға қолданылатын қауіпсіздік сертификатының сілтемелі идентификаторын;

– қауіпсіздік сертификатының топтарын шақыруға қолданылатын қауіпсіздік сертификат топтарының идентификаторын қамтиды.

8.4 Қауіпсіздік маркерлері

Қауіпсіздік маркері – бұл өзара байланысатын мәндер арасында таратылатын және бір немесе бірнеше қауіпсіздік сервистерімен осы қауіпсіздік сервистерін ұсынуға қолданылатын қауіпсіздік ақпаратымен бірге қорғалған деректер топтамасы. Қауіпсіздік маркерлері оларды құрғандығына және қандай қауіпсіздік сервистері олардың мазмұнын қорғайтынына сәйкес сыныпталуы мүмкін.

Қауіпсіздік жөніндегі уәкілмен құрылған және дерек көздерінің тұтастық және сәйкестендіру сервистерімен қорғалған қауіпсіздік маркері қауіпсіздік сертификаты деп аталады (8.3 тармағын қараңыз).

Көптеген қауіпсіздік механизмдері үшін өзара байланысатын қос мәндер арасындағы тұтастықты қорғайтын ақпараттармен алмасу талап етіледі, бұл қос мәндердің ешқайсысы қауіпсіздікке құқылы емес. Тұтастықты қорғайтын ақпараттармен алмасуға қолданылатын қауіпсіздік маркерлері қауіпсіздік сертификаттары болып саналмайды, себебі олардың қосарланған мәндері қауіпсіздікке құқылы емес. Мұндай қауіпсіздік

маркерлері **тұтастықты қорғайтын қауіпсіздік маркерлері** болып табылады.

Тұтастықты қорғайтын барлық қауіпсіздік маркерлері мына ақпаратты қамтиды:

– дерек көздерінің тұтастығы сияқты, сәйкестендіруін қамтамасыз ететін ақпарат (мысалы, криптографиялық бақылау мәні және оны верификаттауға қолданылатын ақпарат көрсеткіші).

– Тұтастықты қорғайтын барлық қауіпсіздік маркерлері мына ақпараттарды қамтиды:

– жарамдылық мерзімі анықталатын ақпарат;

– таратылудан қорғауға қолданылатын ақпарат (мысалы, бірегей нөмір).

9 Қауіпсіздіктің әмбебап құралдары

Көптеген құралдар Қауіпсіздік негіздерінің бірнеше бөлімдеріне талап етіледі. Осы тарауда Қауіпсіздік негіздерінің басқа бөлімдерінде қолданылатын осы құралдар анықталған.

9.1 Басқаруға қатысты құралдар

Осы тарауда басқару құралдарының әмбебап түрлері қарастырылады. Қауіпсіздіктің нақты тетіктеріне сәйкес басқару құралдарының сыныпқа бөлінген тармақтары болуы мүмкін.

9.1.1 ҚА инсталлизациялау

Бұл құрал элементпен байланысты қауіпсіздік ақпараттарының бастапқы топтамасын белгілейді.

9.1.2 ҚА инсталлизациясын ашу

Бұл құрал қауіпсіздік доменіндегі мәннің мүшелігін декларациялайтын ҚА шақыра отырып, қауіпсіздік доменінен мәндердің жойылуын тудырады.

9.1.3 ҚА өзгерту

Бұл құрал элементпен байланысты ҚА түрленуін орындайды.

9.1.4 ҚА бекіту

Бұл құрал ҚА жинағын элементпен байланыстырады. *ҚА бекіту* құралы қауіпсіздік уәкілеттікпен немесе оның агентімен қосылады.

9.1.5 ҚА жарамсыз ету

Бұл құрал элементпен қауымдасатын ҚАның кез келген қолданылуын бұғаттайды. *ҚА жарамсыз ету* құралы қауіпсіздік уәкілімен немесе оның агентімен қосылады. *ҚА жарамсыз ету* құралымен бұғатталған қауіпсіздік

ақпараты аудит және ҚА бұғатталуын қамтамасыз ету мақсатында жүйеде сақталуы мүмкін.

9.1.6 Қауіпсіздік сервисін ажырату/қосу

Бұл құралдар қауіпсіздік сервисінің берілген аспектілерін ажыратып қосады.

9.1.7 Тіркеу

Бұл құрал қауіпсіздік жөніндегі уәкілден мәндерге қауымдасқан кейбір қауіпсіздік ақпараттарын жазуды талап етеді. Тіркеу құралы қауіпсіздік жөніндегі уәкілеттіктен ерекшеленетін мәнмен туындауы мүмкін. Мысалы, қауіпсіздік доменіне кіретін мән қауіпсіздік жөніндегі уәкілдікке қауіпсіздік доменіне кіру ниеті туралы хабарлау үшін тіркеу құралын қолдана алады.

9.1.8 Тіркеуден бас тарту

Бұл құрал элементті қауіпсіздік доменіне шығарылуын және онымен қауымдасқан ҚА шақырылуын тудырады. Бұл құрал қауіпсіздік жөніндегі уәкілеттікпен немесе оның агентімен қосылады. Қауіпсіздік саясаты ҚА кейбір түрлері жойылмауын талап ете алады.

9.1.9 ҚА тарату

Бұл құрал ҚА басқа мәндерге мүмкін болатындай қауіпсіздік уәкілімен немесе оның агентімен қолданылады.

9.1.10 ҚА тізімін құрастыру

Бұл құрал осы элементпен байланысты ҚА тізімін береді.

9.2 Пайдалануға қатысты құралдар

9.2.1 Қауіпсіздік жөніндегі сенімді уәкілді сәйкестендіру

Бұл құрал қауіпсіздіктің нақты элементтері және берілген әрекеттері үшін (мысалы, шифрлеу кілтін ұсыну, кіруді басқару қауіпсіздігінің сертификаты немесе сәйкестендіру қауіпсіздігінің сертификаттары үшін қауіпсіздік саясатының контекстіндегі сенімді болып табылатын қауіпсіздік жөніндегі уәкілді сәйкестендіреді.

9.2.2 Қауіпсіз өзара әрекет ету ережелерін сәйкестендіру

Бұл құрал қолданылатын қауіпсіз өзара байланысу ережелерін сәйкестендіреді. Бұл алдын ала орнатылған ақпарат көмегімен немесе 7.2.4 тармағында мазмұндалғандай домендердің өзара байланысқан элементтері арасындағы келіссөздер арқылы жүзеге асады.

Ескертпе – Қауіпсіз өзара байланысу ережелері осы құралды пайдалану емес, қауіпсіздік домендері арасындағы келісіммен орнатылады. Осы құрал анықталған қауіпсіз өзара байланысу ережелерінің қайсысы нақты әрекетке қолданылатындығын анықтайды.

9.2.3 ҚА жинау

Бұл құрал әрекет ету алдында қауіпсіздік ақпараттарын жинайды. Осы құралдың сынып тармақтары:

– Кіруді басқару: бастамашының кіруді басқару ақпараттарын алу, кіруді басқару ақпаратының мақсаттарын алу.

– Сәйкестендіру: Жинау.

9.2.4 ҚА генерациялау

Бұл құрал қауіпсіздікпен байланысты нақты әрекеттерге арналған ҚА генерациялайды. ҚА деректерге байланысты болуы мүмкін.

Осы құралдың сынып тармақтары:

– Кіруді басқару: кіруді басқару ақпаратын әрекетпен байланыстыру.

– Сәйкестендіру: Генерациялау.

– Істен шықпау: Куәлікті генерациялау.

9.2.5 ҚА верификаттау

Бұл құрал *ҚА генерациялау* құралын шақыру көмегімен туындаған ҚА нақтылығын верификаттайды. *ҚА верификаттау* құралы ҚА верификаттау құралын басқамен шақыратын ҚА туындауына өзі ықпал етеді.

Осы құралдың сынып тармақтары:

– Кіруді басқару: Кіруді басқару ақпаратының әрекетін верификаттау.

– Сәйкестендіру: Верификаттау.

– Істен шықпау: Куәлікті бекіту болып табылады.

ҚА верификаттау құралының қорытындысы одан әрі верификаттауға қайта оралатын жағдайдың мысалы, өзара байланысты сәйкестендірудің екі жақты хаттамасы болып табылады. А және В мәндері бірін-бірі сәйкестендіреді деп болжап көрейік, А хаттамалық алмасуды бастайды. А тұпнұсқалығын құрайтын сәйкестендіру ақпаратын құруға қажет *генерациялау* құралын шақырады және В мәніне қойылатын сұраққа әрине В мәні жауап береді. В мәні А мәнінен сұрақ алынғандығын тексеру үшін *верификаттау* құралын қолданады, сонымен қатар В түпнұсқалығының дәлелдемесін қамтитын сәйкестендіру ақпаратының жаңа элементін құрады және А сұрағына жауап береді. Сосын А мәні В жауабын өңдеу үшін *верификаттау* құралын қолданады. *Верификаттау* құралы жауаптың В алынғандығын және ол бастапқы сұрауға сәйкес екендігін тексереді.

10 Қауіпсіздік тетіктерінің өзара байланысы

Бір байланысу сеансына бірнеше қауіпсіздік сервистері талап етілетіндігі жиі кездеседі. Бұл талап бірнеше қауіпсіздік сервистерін ұсынатын бір қауіпсіздік тетігін қолдану көмегімен немесе біруақытта бірнеше қауіпсіздік сервистерін қолдану көмегімен орындалуы мүмкін.

Кейде, әртүрлі қауіпсіздік тетіктерін біруақытта пайдалану кезінде, бұл тетіктер кері әсер етуі мүмкін, ал бұл өз кезегінде шабуылмен пайдаланылады. Яғни қауіпсіздіктің басым деңгейін қамтамасыз ететін тетіктер жеке-жеке пайдаланылғанда басқа тетіктермен үйлестіріп пайдалану барысында әлсіз болуы мүмкін. Кейде екі қауіпсіздік тетікті бірнеше әртүрлі тәсілдермен біріктіруге болады; біріккен тетіктердің әлсіздігі оларды біріктіру тәсіліне байланысты ерекшеленуі мүмкін.

Тетіктер арасындағы маңызды жағдай екі криптографиялық тетіктерді біріктіру кезінде (мысалы, тұтастық тетікті және құпиялық тетігін немесе істен шықпау тетігі мен құпиялық тетігін біріктіруде) кездеседі. Біріктірілген тетіктердің қауіпсіздік қасиеттері осы екі криптографиялық түрлендірулер қолданылатын тәртіпке байланысты.

Жалпы алғанда, асимметриялық криптографиялық алгоритмдерді пайдалану кезінде, тұтастықты немесе істен шықпауды түрлендіру ашық мәтінге қолданған дұрыс, сосын нәтижелі қол қойылған немесе пломба салынған деректерді шифрлеу керек.

Осы екі сервисті кері тәртіпте пайдалану жағдайының мысалы (яғни, ең алдымен – құпиялық сервисі) сервистер әртүрлі мәндер арасында қолданылатын жағдай болып табылады және бір мәннің ашық мәтінді білу рұқсаты болмаған жағдайда, шифрленген мәтіннің тұтастығын верификаттау мүмкіндігі болуы тиіс. Осыған ұқсас жағдай мәліметтерді тарататын агентке мәліметтің ашық мәтіні қаншалықты екендігін білу рұқсаты болмаған жағдайда мәліметтердің тұтастығын және дереккөздерін тексеру талап етілгенде мәліметтерді өңдеу жүйесінде кездесуі мүмкін.

Құпиялық және тұтастық сервистерін кері тәртіппен пайдалану қауіпті, себебі тұтастық сервисі істен шықпауды қамтамасыз ете алмайды. Егер барлық үш сервис және тұтастық пен құпиялықтың кері тәртібі қажет болса, онда екі тұтастық механизмін пайдалануға болады, біреуі құпиялық механизмін пайдалану алдында, ал екіншісі – пайдаланған кейін қолданылады. Мұндай жағдайлар мәліметтерді өңдеу жүйелерінде кездеседі, мәліметтегі құпиялықты қамтамасыз ету кезінде екі түрлі сандық қолтаңбаларды қолдануға болады (бірігуі шифрленгені анықталады және мәліметтерді тарататын агентпен қолданылады, ал екіншісі алу үшін жіберушінің істен шықпауын қамтамасыз ете отырып, ашық мәтін үшін анықталады.).

11 Қызмет көрсетуден бас тарту және қол жетімділік

Сервиске кіру мүмкін емес жағдайларды қоса алғанда, қызмет көрсетудің істен шығуы қызмет көрсету параметрлерінің мәндері талап етілетін деңгейден төмен болған сайын туындайды. Қызмет көрсетудің істен шығуы мәжбүрлі шабуыл салдарынан немесе боран немесе жер сілкінісі

сияқты, кездейсоқ жағдайларға байланысты туындауы мүмкін. Қол жеткізу — бұл қызмет көрсетудің істен шығуының немесе коммуникация сапасының деградациялауының болмауы.

Қызмет көрсетудің істен шығуына әрдайым кедергі бола алмайсың. Қызмет көрсетудің істен шығуын анықтау үшін түзету шараларын қабылдауға мүмкіндік беретін қауіпсіздік сервистерін қолдануға болады. Мұндай анықтауда шабуыл нәтижесі ме әлде кездейсоқ жағдайлардың салдары ма білу мүмкін бола бермейді. Нақты қауіпсіздік саясаты қызмет көрсетудің істен шығуын анықтау кезінде мұны хаттамалауды (аудит жүргізу мақсатында) және дабыл сигналының процессорына сигнал жіберуді талап етуі мүмкін.

Қызмет көрсетудің істен шыққандығы анықталған соң қауіпсіздік сервистері жағдайды түзету және қызмет көрсетудің қолданымды деңгейіне оралу үшін қолданылуы мүмкін. Бұл анықтау және түзету шаралары басқа сервистердің қауіпсіздік сервисін қолдануды қамтуы мүмкін (мысалы, басқа арналар бойынша трафик маршруты, резервтік процессорларды сақтау немесе қосу резервтік құралдарына ауысу).

«Қызметтің істен шығуы» түріндегі шабуыл көптеген сервис түрлеріне бағытталуы мүмкін және осындай шабуылдарды жоюға қолданылатын механизмдер қорғалатын қолданба түріне байланысты ауытқуы мүмкін. Бұл қызмет көрсетудің істен шығуынан қорғайтын механизмдердің жалпы сыныптамасын жүргізу мүмкін еместігін білдіреді және, сәйкесінше, жеке қауіпсіздік инфрақұрылымдарының сипаттамасы осы механизмдерге қатысты болмайды.

12 Өзге де талаптар

Негіздердің осы бөлімдерінде сипатталған қауіпсіздік шараларынан басқа, шаралар талап етілуі мүмкін (мысалы, физикалық қауіпсіздік және қызметкердің қауіпсіздік шаралары). Осы шараларды қамтамасыз ету үшін қауіпсіздік сервистерін осы стандарт бойынша анықтау мүмкін емес. Осыған ұқсас қосымша қауіпсіздік шараларын қолдану осы негіздерде сипатталған кейбір қауіпсіздік сервистердің қажеттілігін тіпті талап етпеуі мүмкін.

А қосымшасы
(анықтамалық)

Қауіпсіздік сертификаттарын қорғау тетіктерінің кейбір мысалдары

Қауіпсіздік сертификаттарына әлеуетті қауіптілік – бұл шабуылдаушы өзін қауіпсіздік сертификатына сілтеме беретін мән түрінде жалған ұсыну қаупі. Бұл қауіпсіздік сертификатын рұқсатсыз пайдалану қауіпсіздік сертификатын ұрлау деп аталады.

Бұл қауіп сыртқы да, ішкі де болуы мүмкін. Сыртқы қауіп шабуылдаушы өзге тәсілмен кіру мүмкін емес коммуникацияны ұрлап тыңдау арқылы қауіпсіздік сертификатын алу болып табылады. Ішкі қауіп сертификатты заңды түрде алуға құқылы мән өзін сертификатта әрекет ететін мән түрінде жалған ұсыну болып табылады (мысалы, өзі өзара байланысатын ҚА мәнін белгілеу үшін).

Қауіпсіздік сертификаты ТОС коммуникациясының қауіпсіздік сервистерін тікелей пайдалану немесе қауіпсіздік сертификаттары үшін ішкі және сыртқы қосымша параметрлерді талап ететін баламалы қорғау әдісінің көмегімен ұрлықтан қорғалуы мүмкін.

Егер қауіпсіздік сертификатын пайдалануға құқылы мән осы құқықты басқа мәнге бере алса, қауіпсіздік сертификаттарын қорғау механизмі басқаларға өткізілуін қамтамасыз етеді - дейді. Осы қосымшада сипатталған кейбір механизмдер басқаларға өткізілуін қамтамасыз етеді.

А.1 ТОС коммуникациясының қауіпсіздік сервисін қолданатын қорғау

Сыртқы қаскүнем тарапынан ұрлау қаупіне өзара байланысты мәндер арасында қауіпсіздік сертификатын тарату кезінде құпиялылық сервисін қолдану арқылы қарсы тұруға болады.

А.2 Қауіпсіздік сертификатының ішкі параметрлерінің көмегімен қорғау

Қауіпсіздік сертификаттарын ұрлаудан қорғайтын көптеген ұқсас әдістер кездеседі. Осы әдістердің әрқайсысы сертификаттағы ішкі параметрлерге және қауымдасқан сыртқы параметрлерге сүйенеді. Нақты қолданылатын әдістер қауіпсіздік сертификатында көрсетілуі мүмкін.

Осы әдістер қамтиды:

– Сәйкестендіру әдісін;

– Құпиялы кілт әдісін;

– Ашық кілт әдісін;

– Бір тараптық функциялар әдісін.

Қауіпсіздік сертификаты осындай бірнеше әдістердің үйлесімін қолдана алады.

А.2.1 Сәйкестендіру әдісі

Осы әдісте ішкі әдіс сертификат қолдануға рұқсат етілген мәндердің ерекше идентификаторлары болып табылады. Сыртқы параметр сертификатты қолданғысы келетін мәндердің ерекше идентификаторы болып табылады. Осы сыртқы параметр сәйкестендіру сервисімен ұсынылады. Сондай-ақ, сертификат сәйкестендіру процесімен қолданылатын қауіпсіздік сертификатының реттік нөмірі секілді, қосымша параметрлерді қамтуы тиіс.

Сәйкестендіру әдісі мына қауіпсіздік сертификатының қорғалуын қамтамасыз етеді:

– Ол идентификаторлары қауіпсіздік сертификатына енгізілген мәндері бар қауіпсіздік сертификатын пайдалануға жол бермейді.

Бұл әдіс сертификаттың уәкілді пайдаланушысына бұл құқықты басқа мәнге берілуіне жол бермейді, себебі сертификатты қолдануға құқылы мәндер жинағы сертификатты құру барысында белгіленеді. Яғни, бұл әдіс құқықтың таратылуын қамтамасыз етпейді.

А.2.2 Құпия кілт әдісі

Бұл әдісте бүкіл сертификат симметриялық криптографиялық алгоритм көмегімен шифрленеді. Осы әдістегі сыртқы параметр сертификаттың шифрін ашу үшін қолданылатын құпиялы кілт болып табылады.

Құпия кілт әдісі қауіпсіздік сертификатының мынадай қорғалуын қамтамасыз етеді:

– Ол құпия кілттің мәні белгілі (және сәйкесінше, шифрленген сертификаттың шифрін аша алатын) мәндерге ғана қауіпсіздік сертификатын қолдануды болдырмайды.

Бұл әдіс құқықтың берілуін қамтамасыз етеді, себебі сертификаттың уәкілетті пайдаланушысы осы құқықта басқа мәнге тарата алады, ол үшін құпиялы кілтті немесе шифрленген сертификатты беруі тиіс.

А.2.3 Ашық кілт әдісі

Осы әдісте ашық кілт ішкі параметр болып табылады. Сыртқы параметр тиісті жабық кілт болып табылады.

Ашық кілт әдісі қауіпсіздік сертификатын келесі түрде қорғайды:

– Ол жабық кілттің мәні белгілі (және сәйкесінше, жабық кілтті қолданып сандық қолтаңбаны анықтай алатын) мәндерге ғана қауіпсіздік сертификатын қолдануды болдырмайды.

Бұл әдіс құқықтың берілуін қамтамасыз етеді, себебі сертификаттың уәкілетті пайдаланушысы осы құқықта басқа мәнге тарата алады, ол үшін жабық кілтті беруі тиіс.

А.2.4 Бір тараптық қызметтер әдісі

Осы әдісте ішкі параметр сыртқы параметрге бір тараптық қызметті қолдану нәтижесі болып табылады. Ішкі параметр *қорғау кілті*, ал сыртқы параметр *бақылау кілт* деп аталады.

Бір тараптық қызмет әдісі қауіпсіздік сертификатын төмендегідей қорғайды:

– Ол бақылау кілтінің мәні белгілі (және сәйкесінше, оның мәнін ашып оларға бақылау кілтінің белгілі екендігін дәлелдей алатын) мәндерге ғана қауіпсіздік сертификатын қолдануды болдырмайды.

Бұл әдіс құқықтың берілуін қамтамасыз етеді, себебі сертификаттың уәкілетті пайдаланушысы осы құқықта басқа мәнге тарата алады, ол үшін бақылау кілтін беруге тиіс.

А.3 Тарату кезінде ішкі және сыртқы параметрлерді қорғау

Төрт жағдай қарастырылады:

– Ішкі параметрді сертификатты құру алдында сертификатты шығаратын ортада тарату. Бұл ішкі және сыртқы параметрлер сертификаттың шығарылу ортасында генерацияланбаған жағдайда, мүмкін болады.

– Сыртқы параметрді сертификатты құрғаннан кейін сертификат шығаратын ортада тарату. Бұл ішкі және сыртқы параметрлер сертификаттың шығарылу ортасымен генерацияланған жағдайда, мүмкін болады.

– Сыртқы параметрді сертификатты қолдану құқығы расталған жағдайда мәндер арасында тарату.

– Сыртқы параметрді сертификатты қолдану құқығын берген жағдайда мәндер арасында тарату.

А.3.1 Ішкі параметрді сертификат шығарылатын ортаға беру

Сәйкестендіру әдісінде, ашық кілт әдісінде және бір тараптық функция әдісінде қауіпсіздік сертификатына енгізу алдында ішкі параметр қауіпсіздік жөніндегі уәкілге хабарлануы мүмкін. Ішкі параметрді қауіпсіздік жөніндегі уәкілге таратылған жағдайда оның тұтастығы қорғалуы тиіс.

Құпиялы кілт әдісінде қауіпсіздік сертификатын құру алдында сыртқы параметр (яғни құпиялы кілт) қауіпсіздік жөніндегі уәкілге хабарлануы мүмкін. Бұл жағдайда тұтастықты сияқты, құпиялықты да қорғау талап етіледі.

А.3.2 Мәндер арасында сыртқы параметрлерді тарату

Сәйкестендіру әдісінде сыртқы параметр (сертификатты пайдаланушы идентификаторы) сәйкестендіру механизмімен ұсынылады.

Құпиялы кілт әдісінде және бір тараптық функциялау әдісінде сыртқы параметр сертификатты қолдану барысында мәндер арасында таратылуы тиіс. Бұл құпиялы кілттің немесе бақылау кілтінің мәнін білетіндермен қауіпсіздік сертификатын пайдалануды болдырмайды. Мәндер арасында сыртқы параметрді тарату кезінде оның құпиялығы қорғалуы тиіс.

Екі әдіс арасындағы айырмашылық қауіпсіздік сертификатының криптографиялық бақылау мәнін тексергенге дейін құпиялы кілт әдісін қолдану барысында сыртқы параметрдің мәнін ашу болып табылады. Сәйкесінше, бір тараптық функциялау әдісінде қауіпсіздік сертификатының бақылау мәні сыртқы параметрді ашпас бұрын тексерілуі мүмкін.

Сыртқы кілт әдісінде сыртқы параметрді сертификатты пайдалану кезінде мәндер арасында таратудың қажеті жоқ, себебі мән оған жабық кілттің мәнін ашпай-ақ (сандық қолтаңбаны құрып), ол жабық кілттің белгілі екендігін дәлдеуі мүмкін. Осы әдісте сыртқы параметр (жабық кілт) сертификатты пайдалану құқығын өткізген кезде ғана таратылу керек. жабық кілтті тарату барысында мәндер арасында олардың құпиялығы қорғалуы тиіс.

А.4 Жеке мәндермен немесе мәндер тобымен қауіпсіздік сертификаттарын қолдану

Жоғарыда мазмұндалған қорғау әдістері қауіпсіздік сертификатының қолданылуын немесе бір атаулы мәнмен немесе бір атаулы мәндер тобымен шектеу үшін қолданылуы мүмкін:

– Қауіпсіздік сертификаты нақты мәнмен байланысты болуы мүмкін; құпиялы кілт, жабық кілт немесе бақылау кілті шифрленген түрде жалғыз мәнге таратылады және сертификатта ерекше идентификатор немесе осы мәннің қауіпсіздік атрибуттары пайда болады.

– Қауіпсіздік сертификаты атаулы мәндер тобымен байланысты болуы мүмкін; құпиялы кілт, жабық кілт немесе бақылау кілті шифрленген түрде топ мүшелеріне таратылады және сертификатта ерекше идентификатор немесе осы топтың қауіпсіздік атрибуттары пайда болады. Осылайша, топтың кез келген мүшесі қауіпсіздік сертификатын қолдана алады.

А.5 Қауіпсіздік сертификатын кіру мүмкіндігімен байланыстыру

Қауіпсіздік сертификаттарын кіруді басқару үшін қолдануға болады. Бұл жағдайда қауіпсіздік сертификатымен және ол қамтамасыз ететін кіру сұраулары арасында

қорғалған байланыс орнатылуы тиіс. Егер мұнда қорғалған байланыс болмаса, онда қауіпсіздік сертификаты ашып алу шабуылына әлсіз болады және ашып алу шабуылы түпнұсқалы қауіпсіздік сертификатының көшірмесін кіру сұрауын жасанды түрде қолдан жасайды.

Бұл шабуылды қауіпсіздік сертифкатын, сыртқы параметрді және кіру сұрауын бірге байланыстыру үшін тұтастық сервисін қолдану арқылы жоюға болады.

Сәйкестендіру әдісін қолдану кезінде бұл байланысты Сәйкестендіру негіздерінде сипатталғандай ақпараттардың алмасуын сәйкестендіруді тұтастық механизмімен байланыстыру арқылы қол жеткізуге болады (*ҚР СТ ИСО/МЭК 10181-2*).

Құпиялы кілт әдісін қолдану барысында бұл байланыстыру тұтастық механизмінің кілтін қауіпсіздік сертификатының ішіне енгізу және осы кілтті кіру сұрауын пломбалауға қолдану арқылы мүмкін болады. Немесе тұтастық механизмінің кілті ретінде құпиялы кілтті (немесе оның басқа түрін) қолдануға да болады.

Ескертпе – Бір криптографиялық кілтті тұтастық механизмі және құпиялық механизмі үшін қолдану шабуылдың кейбір түрлеріне жол беруі мүмкін. Бұл қауіпті алдын алу үшін кілт нұсқалары қолданылуы мүмкін. Криптографиялық кілт нұсқасы – бұл бастапқы кілттен алынған, бірақ бастапқы кілт болып саналмайтын, басқа криптографиялық кілт.

Бір тараптан функциялау әдісін қолдану барысында осы байланыстыру бақылау кілтін бір тараптан функциялауға негізделген тұтастық механизмінің кілті ретінде қолдану арқылы мүмкін болады.

Ашық кілт әдісін қолдану кезінде бұл байланыстыруға кіру сұрауына қол қоюға талап етілетін жабық кілтті қолдану арқылы қол жеткізуге болады.

Осы барлық әдістерде қауіпсіздік сертификатын, сыртқы параметрді және кіру сұрауын байланыстыруға ТОС коммуникациясының сервистік бөлімі ретінде ұсынылатын тұтастық сервисін қолдану арқылы қол жеткізуге болады.

ӘОЖ 681.324:006.354 **МСЖ 35.100**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, желілердің өзара байланысы, ашық жүйелердің өзара байланысы, коммуникациялық процедуралар, ақпаратты қорғау, қауіпсіздік технологиялары, шолу.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ

Основы безопасности для открытых систем

Часть 1

Обзор

СТ РК ИСО/МЭК 10181-1-2008
(ИСО/МЭК 10181-1:1996 «Информационная технология. Взаимодействие открытых систем Основы безопасности для открытых систем. Часть 1 Обзор», IDT)

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 10181-1:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем: Обзор» («Information technology. Open Systems Interconnection. Security frameworks for open systems: Overview»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ ОСНОВЫ БЕЗОПАСНОСТИ ДЛЯ ОТКРЫТЫХ СИСТЕМ Часть 1 Обзор

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает Основы безопасности, предназначенные для решения задачи применения сервисов безопасности в среде открытых систем. Под термином «Открытые системы» понимаются такие области, как базы данных, распределенные приложения, открытая распределенная обработка данных и взаимодействие открытых систем.

Основы безопасности оперируют как с элементами данных, так и с последовательностями действий (но не элементами протоколов), используемыми для получения специфических сервисов безопасности. Эти сервисы безопасности могут применяться как к взаимодействующим объектам систем, так и к обмену данными между системами, а также к данным, которыми управляют системы.

Основы безопасности являются базой дальнейшей стандартизации, предоставляя согласованную терминологию и определения универсальных абстрактных интерфейсов сервисов для конкретных требований безопасности. Они также классифицируют механизмы, которые могут быть использованы для выполнения этих требований.

Зачастую один сервис безопасности зависит от других сервисов, что затрудняет выделение отдельных частей системы безопасности. Основы безопасности имеют дело с конкретными сервисами безопасности, описывают спектр механизмов, которые могут быть использованы для предоставления сервисов безопасности, и определяют взаимосвязи между сервисами и механизмами. Описание этих механизмов может опираться на другой сервис безопасности, и именно таким образом Основы безопасности описывают, как один сервис безопасности используется другим.

Некоторые сервисы безопасности, используемые в настоящем стандарте, базируются на применении криптографических методов. Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан и не является предметом рассмотрения настоящего стандарта.

Настоящий стандарт устанавливает:

– организацию Основ безопасности;

– определение понятий безопасности, используемые в нескольких частях Основ безопасности;

– взаимосвязи сервисов и механизмов, определяемых в других частях Основ.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ИСО/МЭК 9798-2008 Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации сущностей. Часть 1. Общая модель.

СТ РК ИСО/МЭК 10181-2-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы аутентификации.

СТ РК ИСО/МЭК 10181-3-2008 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы управления доступом.

СТ РК ИСО/МЭК 11770-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 1. Основы управления ключами.

ГОСТ ИСО 7498-2-2002 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

ИСО/МЭК 7498-1-1994 Информационные технологии. Взаимодействие открытых систем. Основная эталонная модель: Основная модель.

ИСО/МЭК 9594-8-1995 Информационная технология. Взаимодействие открытых систем. Справочники: Основы аутентификации.

3 Термины и определения

В настоящем стандарте применены термины по *ИСО/МЭК 7498-1*, ГОСТ ИСО 7498-2, а также следующие термины с соответствующими определениями:

3.1 Администратор безопасности (security administrator) - лицо, отвечающее за определение или проведение в жизнь одной или нескольких частей политики безопасности.

3.2 Асимметричный криптографический алгоритм (asymmetric cryptographic algorithm) - алгоритм для зашифрования или соответствующего расшифрования, в котором ключи зашифрования и расшифрования различаются.

Примечание. В некоторых криптографических алгоритмах для расшифрования или генерации цифровой подписи требуется несколько закрытых ключей.

3.3 Безусловно доверенная сущность (unconditionally trusted entity) - доверенная сущность, которая может нарушать политику безопасности, оставаясь необнаруженной.

3.4 Восстановление безопасности (security recovery) - предпринимаемые действия и выполняемые процедуры, если обнаружено или подозревается нарушение безопасности.

3.5 Доверенная сущность (trusted entity) - сущность, которая может нарушать политику безопасности, либо выполняя действия, которых от нее не ожидают, либо неудачно выполняя ожидаемые действия.

3.6 Доверенная третья сторона (trusted third party) - уполномоченный по безопасности или его агент, которым доверяют в рамках некоторых связанных с безопасностью действий (в контексте политики безопасности).

3.7 Доверие (trust). Говорят, что сущность X доверяет сущности Y в рамках некоторого набора действий, тогда и только тогда, когда сущность X полагается на надлежащее поведение сущности Y в этих рамках.

3.8 Домен безопасности (security domain) - набор элементов, политика безопасности, уполномоченный по безопасности и набор действий, связанных с безопасностью, в которых набор элементов является субъектом политики безопасности для заданных действий, а политика безопасности администрируется уполномоченным по безопасности данного домена безопасности.

3.9 Закрытый ключ (private key) - ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно допускается только для одной сущности).

3.10 Информация безопасности (security information) - информация, необходимая для реализации сервисов безопасности.

3.11 Криптографическое сцепление (cryptographic chaining) - режим использования криптографического алгоритма, при котором преобразование, выполняемое алгоритмом, зависит от значений предыдущих входных или выходных данных.

3.12 Маркер безопасности (security token) - набор данных, защищенный одним или несколькими сервисами безопасности, вместе с информацией безопасности, используемой при предоставлении данных сервисов безопасности, который передается между взаимодействующими сущностями.

3.13 Односторонняя функция (one-way function) - функция (математическая), которую легко вычислить, но при известном результате вычислительно неосуществимо найти какое-либо значение, которое могло быть использовано для получения данного результата.

3.14 Односторонняя хэш-функция (one-way hash function) - функция (математическая), которая одновременно является и односторонней, и хэш-функцией.

3.15 Открытый ключ (public key) - ключ, который используется в асимметричном криптографическом алгоритме и может быть сделан общедоступным.

3.16 Отличительный идентификатор (distinguishing identifier) - данные, уникальным образом идентифицирующие сущность.

3.17 Пломба (seal) - криптографическое контрольное значение, поддерживающая целостность, но не защищающая от подделки получателем (т.е. не обеспечивающая неотказуемость). Если пломба ассоциирована с элементом данных, то говорят, что элемент данных опломбирован.

Примечание. Хотя пломба сама по себе не обеспечивает неотказуемость, некоторые механизмы неотказуемости используют сервис целостности, обеспечиваемую пломбами, например, для защиты коммуникаций с доверенными третьими сторонами.

3.18 Правила безопасного взаимодействия (secure interaction rules) - правила политики безопасности, регулирующие взаимодействие между доменами безопасности.

3.19 Правила политики безопасности (security policy rules) - представление политики безопасности для домена безопасности в рамках реальной системы.

3.20 Секретный ключ (secret key) - ключ, используемый в симметричном криптографическом алгоритме. Обладание секретным ключом ограничено (обычно до двух сущностей).

3.21 Сертификат безопасности (security certificate) - набор связанных с безопасностью данных, выпущенный уполномоченным по безопасности или доверенной третьей стороной, вместе с информацией безопасности, используемый для предоставления сервисов целостности и аутентификации источника данных.

Примечание. Все сертификаты считаются сертификатами безопасности (см. соответствующие определения в ГОСТ ИСО 7498-2). Термин «сертификат безопасности» используется, чтобы избежать терминологических конфликтов с ИСО/МЭК 9594-8 (Основы аутентификации).

3.22 Сертификат отзыва (revocation certificate) - сертификат безопасности, выпущенный удостоверяющим центром и извещающий об отзыве определенного сертификата безопасности.

3.23 Сертификат списка отзыва (revocation list certificate) - сертификат безопасности, в котором приведен список отозванных сертификатов безопасности.

3.24 Симметричный криптографический алгоритм (symmetric cryptographic algorithm): Алгоритм для зашифрования или соответствующего расшифрования, в котором для зашифрования и расшифрования требуется один и тот же ключ.

3.25 Удостоверяющий центр (certification authority) - сущность, которой доверено (в контексте политики безопасности) создавать

сертификаты безопасности, содержащие один или несколько классов данных, связанных с безопасностью.

3.26 Уполномоченный по безопасности (security authority) - сущность, отвечающая за определение, реализацию или проведение в жизнь политики безопасности.

3.27 Уполномоченный по домену безопасности (security domain authority) - уполномоченный по безопасности, отвечающий за реализацию политики безопасности в домене безопасности.

3.28 Условно доверенная сущность (conditionally trusted entity) - сущность, доверенная в контексте политики безопасности, которая не может, оставаясь необнаруженной, нарушать политику безопасности.

3.29 Хэш-функция (hash function) - функция (математическая), которая отображает (возможно, очень) большое множество значений на меньший диапазон значений.

3.30 Цепочка сертификатов безопасности (security certificate chain) - упорядоченная последовательность сертификатов безопасности, в которой первый сертификат содержит связанную с безопасностью информацию, а каждый последующий — информацию безопасности, которая может быть использована при верификации предыдущих сертификатов.

3.31 Цифровой отпечаток (digital fingerprint) - характеристика элемента данных, такая как криптографическое контрольное значение или результат вычисления односторонней хэш-функции для данных, которая специфицирована для элемента данных таким образом, чтобы было вычислительно невозможно найти другой элемент данных, обладающий такими же характеристиками.

4 Сокращения

В настоящем стандарте используются следующие сокращения:

4.1 ИУД - Информация управления доступом;

4.2 ВОС - Взаимодействие открытых систем;

4.3 ОРО - Открытая распределенная обработка;

4.4 ИБ - Информация безопасности;

4.5 ДТС - Доверенная третья сторона.

5 Обозначения

Используемые обозначения уровней совпадают с обозначениями, определенными в [1].

Термин сервис, если не оговорено иное, используется для обозначения сервиса безопасности.

Термин сертификат, если не оговорено иное, используется для обозначения сертификата безопасности.

6 Структура стандарта

Основы безопасности являются частями составного настоящего стандарта и описываются ниже. В будущем набор рассматриваемых Основ безопасности может быть расширен. Основы управления ключами не является частью настоящего стандарта, но имеет аналогичную область применения и их описание включено в целях полноты изложения.

6.1 Часть 1. Обзор

См. раздел 1.

6.2 Часть 2. Аутентификация

Эти Основы описывают все аспекты аутентификации в применении к открытым системам, связь аутентификации с другими функциями обеспечения безопасности, такими как управление доступом, а также требования управления для аутентификации.

Эти Основы определяют:

а) основные понятия аутентификации;

б) возможные классы механизмов аутентификации;

в) сервисы для этих классов механизмов аутентификации;

г) функциональные требования к протоколам для поддержки этих классов механизмов аутентификации;

д) общие требования управления для аутентификации.

Основы аутентификации находятся на верху иерархии стандартов аутентификации, содержащих понятия, перечень и классификацию методов аутентификации. Уровнем ниже располагаются такие стандарты, как *СТ РК ИСО/МЭК 9798-2008 (Механизмы аутентификации)*, содержащие более детальное описание конкретного набора этих методов. Наконец, стандарты, находящиеся в самом низу иерархии, такие как ИСО/МЭК 9594-8 (Основы аутентификации), используют эти понятия и методы в контексте конкретного приложения или требования.

Основы аутентификации описывают модель аутентификации, ряд стадий, на которые разбиваются действия по аутентификации, использование доверенной третьей стороны, применение сертификатов аутентификации для обмена информацией аутентификации, универсальный сервис аутентификации, основанный на этих стадиях, а также, по крайней мере, пять классов механизмов аутентификации, предоставляющих универсальный сервис аутентификации. В их число входят механизмы, предотвращающие раскрытие информации аутентификации, а также раскрытие и повторное использование тех же (и/или других) верификаторов.

6.3 Часть 3. Управление доступом

Эти Основы описывают все аспекты управления доступом (например, доступа пользователя к процессам, пользователя к данным, процесса к процессу, процесса к данным) в открытых системах, взаимосвязи с другими сервисами безопасности, такими как аутентификация и аудит, а также требования управления для осуществления контроля доступа.

Эти Основы:

а) определяют основные понятия управления доступом;

б) демонстрируют, как основные понятия управления доступом могут быть конкретизированы для поддержки некоторых общепризнанных сервисов и механизмов управления доступом;

в) определяют эти сервисы и соответствующие механизмы управления доступом;

г) определяют функциональные требования к протоколам для поддержки этих сервисов и механизмов управления доступом;

д) определяют требования управления для поддержки этих сервисов и механизмов управления доступом.

е) обслуживают взаимодействие сервисов и механизмов управления доступом с другими сервисами и механизмами безопасности.

Эти Основы безопасности описывают модель управления доступом, ряд стадий, на которые разбиваются действия по управлению доступом, универсальный сервис управления доступом, основанный на этих стадиях, и, по крайней мере, три класса механизмов управления доступом, предоставляющих универсальный сервис управления доступом.

6.4 Часть 4. Неотказуемость

Эти Основы уточняют и расширяют концепцию сервисов неотказуемости, описанную в ГОСТ ИСО 7498-2, создавая основы для разработки и предоставления этих сервисов.

Эти Основы:

а) определяют основные понятия неотказуемости;

б) определяют общие сервисы неотказуемости;

в) идентифицируют возможные механизмы для предоставления сервисов неотказуемости;

г) идентифицируют общие требования управления для механизмов и сервисов неотказуемости.

6.5 Часть 5. Конфиденциальность

Назначением сервиса конфиденциальности является защита информации от несанкционированного раскрытия. Эти Основы

предназначены для обеспечения конфиденциальности информации при выборке, передаче и управлении.

Эти Основы:

а) определяют основные понятия;

б) идентифицируют возможные классы механизмов конфиденциальности;

в) определяют возможности каждого класса механизмов конфиденциальности;

г) идентифицируют возможности управления, необходимые для поддержки классов механизмов конфиденциальности;

д) обслуживают взаимодействие механизмов конфиденциальности и вспомогательных сервисов с другими сервисами и механизмами безопасности.

Некоторые процедуры, описанные в этих Основах безопасности, обеспечивают конфиденциальность с помощью криптографических методов. Применение данных Основ не зависит от использования конкретных криптографических или иных алгоритмов, хотя некоторые классы механизмов конфиденциальности могут зависеть от свойств конкретного алгоритма.

6.6 Часть 6. Целостность

Свойство, состоящее в отсутствии несанкционированного изменения или разрушения данных, называется целостностью. Эти Основы предназначены для обеспечения целостности данных при выборке и передаче информации и управлении ею.

Эти Основы:

а) определяют основные понятия целостности;

б) идентифицируют возможные классы механизмов целостности;

в) определяют возможности каждого класса механизмов целостности;

г) идентифицируют возможности управления, необходимее для поддержки классов механизмов целостности;

д) обслуживают взаимодействие механизмов целостности и вспомогательных сервисов с другими сервисами и механизмами безопасности.

Некоторые процедуры, описанные в этих Основах безопасности, обеспечивают целостность с помощью криптографических методов. Применение Основ не зависит от использования конкретных криптографических или иных алгоритмов, хотя некоторые классы механизмов целостности могут зависеть от свойств конкретного алгоритма.

Целостность в контексте этих Основ определяется как постоянство значения данных, а не как постоянство информации, которая, как

предполагается, представлена этими данными. Другие формы неизменности исключаются.

6.7 Часть 7. Аудит безопасности и тревожная сигнализация

Эти Основы:

а) определяют основные понятия аудита безопасности и тревожной сигнализации;

б) предоставляют общую модель аудита безопасности и тревожной сигнализации;

в) идентифицируют взаимодействие сервиса аудита безопасности и тревожной сигнализации с другими сервисами безопасности.

Как и другие сервисы безопасности, аудит безопасности может быть обеспечен только в контексте определенной политики безопасности. Политика безопасности определяется уполномоченными по безопасности в пределах их доменов безопасности. Любой стандарт, специфицирующий механизмы, базирующихся на этих Основах, должен уметь поддерживать различные политики безопасности.

6.8 Управление ключами

Основные положения управления ключами (*СТ РК ИСО/МЭК 11770-2008*, часть 1) имеет особые связи с остальными Основами безопасности, поскольку она затрагивает функции, не связанные непосредственно с сервисами безопасности, определенными в *ГОСТ ИСО 7498-2*. Эти функции применимы в любой среде информационных технологий, где уместны шифрование или цифровая подпись.

Эти Основы:

а) идентифицируют цели управления ключами;

б) описывают общие модели, лежащие в основе механизмов управления ключами;

в) определяют основные понятия управления ключами, общие для всех частей данного составного стандарта;

г) определяют сервисы управления ключами;

д) идентифицируют характеристики механизмов управления ключами;

е) специфицируют требования к управлению ключевым материалом на протяжении его жизненного цикла;

ж) описывают основные положения управления ключевым материалом на протяжении его жизненного цикла.

7 Общие понятия

Многие понятия требуются более чем в одной части Основ безопасности. Настоящая часть стандарта определяет эти понятия для последующего использования в оставшихся частях настоящего стандарта.

7.1 Информация безопасности

Информация безопасности (ИБ) – это информация, которая необходима для реализации сервисов безопасности. Примерами информации безопасности являются:

– правила политики безопасности;

– информация для реализации конкретных сервисов безопасности, такая как информация аутентификации (ИА) и информация управления доступом (ИУД);

– информация, относящаяся к механизмам безопасности, такая как метки безопасности, криптографические контрольные значения, сертификаты безопасности и маркеры безопасности.

Типы ИБ, общие для нескольких Основ безопасности, обсуждаются в разделе 8.

7.2 Домен безопасности

Домен безопасности представляет собой набор элементов, подчиненных заданной политике безопасности, администрируемой одним уполномоченным по безопасности для группы конкретных связанных с безопасностью действий. Действия в домене безопасности производятся над одним или несколькими элементами этого домена безопасности и, возможно, элементами других доменов безопасности.

Примерам действий являются:

– доступ к элементам;

– установление или использование соединений ВОС (N)-уровня;

– операции, связанные с конкретной функцией управления;

– операции неотказуемости, включающие нотариат.

Действие может быть связано с безопасностью, даже если оно в данный момент не является субъектом механизмов, которые могли бы проводить в жизнь произвольную политику их использования. В частности, действия, которые нельзя предотвратить в рамках некоторой группы элементов, могут быть связаны с безопасностью и в будущем могут стать субъектами механизмов управления.

Примерами элементов домена безопасности в среде открытых систем являются логические или физические элементы, такие как реальные открытые системы, прикладные процессы, (N)-сущности, (N)-протокольные блоки данных, ретрансляторы и люди-пользователи реальных открытых

систем. Иногда людей-пользователей необходимо отличать от других элементов домена безопасности. В подобных случаях для выделения объектов, не являющихся людьми, будет использован термин «объекты данных».

7.2.1 Политика безопасности и правила политики безопасности

Политика безопасности выражает требования безопасности для домена безопасности в общем виде. Например, политика безопасности может определять требования для всех членов домена безопасности при работе в определенных условиях или для всей информации в домене безопасности. Реализация политики безопасности приведет к идентификации удовлетворяющих ей сервисов безопасности, для реализации которых будут выбраны механизмы безопасности. Решение о выборе механизмов безопасности зависит от предполагаемых угроз и ценности защищаемых ресурсов.

Политика безопасности обычно формулируется на естественном языке в виде общих принципов. Эти принципы отражают требования безопасности для конкретной организации или членов домена безопасности. До того, как эти требования безопасности смогут быть отражены в реальной системе, политика безопасности должна быть уточнена настолько, чтобы из нее можно было вывести набор правил политики безопасности. Интерпретация этих требований в виде правил политики безопасности является техническим действием. Политика безопасности ограничивает действия элементов, являющихся ее субъектами, либо требуя, либо запрещая выполнение определенных действий. Политика безопасности может также разрешать элементам принимать участие в определенных действиях. Такая интерпретация политики безопасности шире, чем в *ГОСТ ИСО 7498-2*, где рассматривается только ВОС. Аспекты политики безопасности, специфичные для конкретного сервиса безопасности, обсуждаются при рассмотрении Основ безопасности для этого сервиса.

Существует два типа правил политики безопасности для домена безопасности: для внутридоменных и междоменных действий. Правила политики безопасности второго типа называются правилами безопасного взаимодействия. Политика безопасности может также определять, какие правила применяются для связей со всеми, а какие — с конкретными доменами безопасности.

Должна поддерживаться актуальность правил политики безопасности для домена безопасности при изменении системы или модификации действий и политики безопасности для домена безопасности.

Примечание. Эти Основы не затрагивают следующие аспекты политики безопасности:

- сторона, самостоятельно устанавливающая или поддерживающая политику безопасности;

- процедуры установления или поддержки политики безопасности;
- содержание политики безопасности;
- процедуры привязки политики безопасности к домену безопасности.

7.2.2 Уполномоченный по домену безопасности

Уполномоченный по домену безопасности — это уполномоченный по безопасности, отвечающий за реализацию политики безопасности для домена безопасности.

Уполномоченный по домену безопасности:

– может быть составной сущностью, такая сущность должна быть идентифицируемой;

– может, в зависимости от политики безопасности, субъектом которой уполномоченный по домену безопасности может являться, делегировать ответственность за реализацию политики безопасности одной или нескольким сущностям;

– обладает полномочиями по отношению к элементам домена безопасности.

Примечание. Политика безопасности может быть пустой, если уполномоченный по домену безопасности решил не налагать никаких ограничений.

Уполномоченные по двум доменам безопасности связаны, если они вынуждены координировать свои политики безопасности.

7.2.3 Взаимосвязи между доменами безопасности

Понятие домена безопасности представляется важным по следующим двум причинам:

– оно может использоваться, чтобы описать, как безопасность управляется и администрируется;

– оно может использоваться как строительный блок при моделировании действий, связанных с безопасностью и включающих элементы, находящиеся под управлением разных уполномоченных по безопасности.

Домены безопасности могут быть связаны одним или несколькими способами. Здесь обсуждаются некоторые возможные взаимосвязи доменов безопасности. Взаимосвязи между доменами безопасности должны быть отражены в политиках безопасности доменов безопасности в виде, согласованном их уполномоченными по безопасности. Эти взаимосвязи формулируются в терминах элементов и действий доменов безопасности и отражаются в правилах безопасного взаимодействия для каждого из взаимосвязанных доменов безопасности. Некоторые конкретные взаимосвязи доменов безопасности описываются в последующей части данного подраздела. Возможно и множество других взаимосвязей доменов безопасности.

а) Два домена безопасности называются **изолированными**, если у них нет общих объектов данных и общих действий, и, следовательно, они не могут взаимодействовать.

б) Два домена безопасности называются **независимыми** друг от друга, если

1) у них нет общих объектов данных;

2) действия внутри каждого домена безопасности подчиняются только их собственным политикам безопасности (и соответствующим наборам правил политики безопасности);

3) уполномоченные по безопасности доменов безопасности не обязаны координировать их политики безопасности.

Два или несколько независимых доменов безопасности могут принять решение о заключении соглашения о координации совместного использования информации (см. 7.2.4).

в) Домен безопасности А называется **поддоменом безопасности** другого домена безопасности В тогда и только тогда, когда:

1) множество элементов А является подмножеством множества элементов В или совпадает с ним;

2) множество действий А является подмножеством множества действий В или совпадает с ним;

3) юрисдикция над А делегирована уполномоченным по безопасности В уполномоченному по безопасности А;

4) политика безопасности А не противоречит политике безопасности В. А может вводить дополнительную политику безопасности, если это необходимо и разрешено политикой безопасности В.

Примечание. Подмножество может совпадать со всем множеством. Как одна из крайностей, поддомен безопасности может быть сформирован из всего множества элементов наддомена безопасности для некоторых классов действий или, как другая крайность, — из всех классов действий для некоторого подмножества из множества элементов наддомена безопасности. Между этими двумя крайностями может существовать множество промежуточных вариантов.

г) Домен безопасности А называется **наддоменом безопасности** другого домена В тогда и только тогда, когда В является поддоменом безопасности А.

Примечание. Настоящие Основы безопасности не требуют, чтобы понятия изолированного, независимого поддомена и наддомена поддерживались какими-либо конкретными протоколами, спецификациями или реализациями.

7.2.4 Установление правил безопасного взаимодействия

Чтобы информационный обмен между доменами безопасности был возможен, для этого обмена должен существовать согласованный набор правил политики безопасности, называемых правилами безопасного взаимодействия. Для каждого домена безопасности они являются частью

правил политики безопасности. Правила безопасного взаимодействия позволяют выбирать общие сервисы и механизмы безопасности, возможно, путем переговоров и ассоциированные элементы информации безопасности в каждом из взаимосвязанных доменов безопасности, возможно, путем отображения. Домены безопасности могут обмениваться информацией управления безопасностью, необходимой для поддержки правил безопасного взаимодействия. В зависимости от взаимосвязей между доменами безопасности правила безопасного взаимодействия могут определяться различными способами.

Для безопасного взаимодействия между независимыми доменами безопасности правила безопасного взаимодействия должны быть согласованы уполномоченными по безопасности взаимодействующих доменов безопасности.

Для безопасного взаимодействия между поддоменами безопасности правила безопасного взаимодействия могут быть установлены уполномоченными по безопасности наддомена безопасности. Если позволяет политика безопасности наддомена безопасности, поддомены безопасности могут устанавливать собственные правила безопасного взаимодействия.

7.2.5 Передача информации безопасности между доменами.

Правила безопасного взаимодействия сами могут задавать информацию безопасности и может требоваться передача этой информации между доменами безопасности. Рассматриваются следующие случаи:

– Семантика и представление информации безопасности идентичны во всех доменах безопасности. Это означает, что трансляции не требуется.

– Семантика информации безопасности идентична во всех доменах безопасности, но ее представления различаются. Это означает, что способы описания информации безопасности различны, и поэтому требуется синтаксическая трансляция.

– И семантика, и представление информации безопасности различны во всех доменах безопасности. Это означает, что правила безопасного взаимодействия должны определять, как информация безопасности одного домена будет транслироваться в информацию безопасности другого домена. Может также потребоваться синтаксическая трансляция.

7.3 Рассмотрение политики безопасности для конкретных сервисов безопасности

В некоторых реализациях сервиса целостности или сервиса конфиденциальности могут использоваться механизмы управления доступом. В подобных случаях правила политики безопасности, касающиеся реализации сервиса целостности или сервиса конфиденциальности, должны описывать, как будут использоваться механизмы управления доступом.

Механизмы управления доступом описываются в терминах инициаторов и целей (в *СТ РК ИСО/МЭК 10181-3-2008*). Правила политики безопасности определяют, как в механизмах управления доступом с инициаторами и целями связаны сущности, информация и элементы данных политик целостности и конфиденциальности.

Политики конфиденциальности формулируются в терминах, в которых сущности могут опрашивать элементы информации. Существует два пути, по которым действие, выполняемое инициатором над целью, может раскрыть информацию для сущности. Во-первых, результат действия может дать инициатору некоторую информацию о цели. Во-вторых, запрос действия может дать цели некоторую информацию об инициаторе. Когда механизмы управления доступом используются для предоставления сервисов конфиденциальности, сущности, пытающиеся получить информацию, считаются инициаторами, а элементы информации считаются целями.

Политики целостности формулируются в терминах, в которых сущности могут изменять элементы данных. Существует два пути, по которым действие, выполняемое инициатором над целью, может привести к изменению данных. Во-первых, действие может непосредственно вызвать изменение данных, содержащихся в цели. Во-вторых, результат действия может вызвать изменение данных, содержащихся в инициаторе. Когда механизмы управления доступом используются для предоставления сервисов целостности, сущности, пытающиеся изменить данные, считаются инициаторами, а элементы данных считаются целями.

7.4 Доверенные сущности

Сущность называется **доверенной сущностью** для некоторых классов действий в контексте политики безопасности, если сущность может нарушать политику безопасности, либо, выполняя действия, которых от нее не ожидают, либо неудачно выполняя ожидаемые действия. Политика безопасности определяет, какие сущности являются доверенными, и для каждой доверенной сущности определяет набор действий, для которых сущность является доверенной. Сущность, являющаяся доверенной для некоторого набора действий, не обязательно является доверенной для всех действий внутри домена безопасности.

Декларирование в политику безопасности того, что сущность должна вести себя определенным образом, не гарантирует соответствующего поведения сущности. Следовательно, политика безопасности может потребовать наличия средств обнаружения нарушений политики безопасности, вызванных ненадлежащим поведением доверенной сущности. Доверенная сущность, ненадлежащее поведение которой не может быть обнаружено, называется **безусловно доверенной сущностью**. Доверенная

сущность, которая может нарушать политику безопасности, но не может при этом остаться необнаруженной, называется **условно доверенной сущностью**.

Доверенная сущность может быть безусловно доверенной для подмножества своих действий, и в то же время — условно доверенной для другого подмножества своих действий. Такая сущность может незаметным образом нарушать некоторые аспекты политики безопасности, но не может нарушать другие аспекты политики безопасности, оставаясь необнаруженной.

Политика безопасности домена безопасности может декларировать, что элемент, не входящий в домен безопасности, является доверенным для некоторого множества действий внутри домена безопасности. Правила безопасного взаимодействия (см. п. 7.2.4) могут определять, как внутренние сущности домена безопасности должны взаимодействовать с доверенной сущностью, внешней для домена безопасности.

7.5 Доверие

Говорят, что сущность X доверяет сущности Y в рамках некоторого набора действий, тогда и только тогда, когда сущность X полагается на надлежащее поведение сущности Y в этих рамках.

Доверие не обязательно взаимно. Сущность, не являющаяся доверенной сущностью, может использовать сервисы, предоставляемые доверенной сущностью. Примером ситуации, когда доверие взаимно, является случай, когда две доверенные сущности сотрудничают при выполнении действия, и каждая из них полагается на помощь другой при проведении в жизнь политики безопасности.

Доверие не обязательно транзитивно. В конкретных случаях политика безопасности может определить транзитивность отношения доверия. Если сущность A полагается на сервисы, предоставляемые доверенной сущностью B, а доверенная сущность B полагается на сервисы, предоставляемые доверенной сущностью C, то A неявно полагается на то, что C ведет себя особенным образом. В случае если это действительно так, доверие транзитивно. Однако в других ситуациях B может принимать меры, гарантирующие, что ненадлежащее поведение C не повлияет на действия A. В таком случае доверие не является транзитивным.

7.6 Доверенные третьи стороны

Доверенная третья сторона – это уполномоченный по безопасности или его агент, являющийся доверенным (в контексте политики безопасности) по отношению к некоторым связанным с безопасностью действиям.

Примерами доверенных третьих сторон служат:

– доверенная третья сторона при аутентификации;

– нотариат или сервис постановки временных штампов для неотказуемости;

– центр распределения ключей при управлении ключами.

8 Универсальная информация безопасности

Некоторые типы информации безопасности требуются при описании нескольких Основ безопасности. В данном разделе описываются эти типы информации безопасности.

Механизмы безопасности, описанные в Основах безопасности, обычно включают обмен информацией безопасности либо между сущностями, которым для взаимодействия необходимы сервисы безопасности, либо между уполномоченным по безопасности и взаимодействующими сущностями. Механизмами, описанными в этих Основах, используются четыре общих формы информации безопасности:

– метки безопасности, используемые для указания политики безопасности, применимой к элементу, каналу связи или единице данных;

– криптографические контрольные значения, используемые для обнаружения изменений единицы данных;

– сертификаты безопасности, используемые для защиты информации безопасности, полученной от уполномоченного по безопасности или ДТС для использования одной или несколькими взаимодействующими сторонами;

– маркеры безопасности, используемые для защиты информации безопасности, передаваемой между взаимодействующими сторонами.

Примечание. Информация безопасности может быть защищена несколькими различными механизмами безопасности. Некоторые механизмы безопасности основываются на использовании криптографии, другие используют физические средства.

8.1 Метки безопасности

Метка безопасности – это набор атрибутов безопасности, связанный с элементом, каналом связи или единицей данных. Метка безопасности также указывает, явно или неявно, на уполномоченного по безопасности, отвечающего за создание связывания и политики безопасности, применимой для использования метки. Метка безопасности может быть использована для поддержки комбинации сервисов безопасности.

Примерами использования меток безопасности служат:

– поддержка основанной на метках безопасности схемы управления доступом, включающей применение управления доступом для обеспечения целостности и/или конфиденциальности;

– указание степени доверия, которое может оказываться данным, и требований по их обработке;

– указание чувствительности данных и требований по их обработке;

– указание требований по защите, расположению и других требований по обращению.

8.2 Криптографическое контрольное значение

Криптографическое контрольное значение — это информация, которая выводится путем выполнения криптографического преобразования блока данных. Тремя примерами криптографических контрольных значений служат пломбы, цифровые подписи и цифровые отпечатки.

Пломба представляет собой форму криптографического контрольного значения, вычисляемую с помощью симметричного криптографического алгоритма и секретного ключа, общего для общающихся сущностей. Пломбы используются для обнаружения изменения данных при передаче.

Цифровая подпись – это криптографическое контрольное значение, защищающее от подделки получателем и вычисляемое с использованием закрытого ключа и асимметричного криптографического алгоритма. Проверка цифровой подписи требует использования этого же криптографического алгоритма и соответствующего открытого ключа.

Примечание.

1. Хотя существуют и другие средства, не позволяющие получателю подделать криптографическое контрольное значение (например, использование криптографических модулей, устойчивых к вмешательству в их работу), в Основах безопасности термин "цифровая подпись" используется для обозначения криптографического контрольного значения, полученного посредством асимметричного криптографического алгоритма.

2. В некоторых асимметричных криптографических алгоритмах вычисление цифровой подписи требует использования нескольких закрытых ключей. При использовании подобных алгоритмов обладание каждым из закрытых ключей может быть позволено только различным сущностям. Это гарантирует, что сущности должны объединиться для создания цифровой подписи.

Цифровой отпечаток — это характеристика элемента данных, достаточно специфичная для данных, чтобы было вычислительно неосуществимо найти другой элемент данных с таким же цифровым отпечатком. В качестве цифрового отпечатка могут быть использованы некоторые формы криптографических контрольных значений (например, результат применения к данным односторонней функции). Цифровые отпечатки могут быть получены и другими способами, отличными от криптографических алгоритмов. Например, цифровым отпечатком является копия элемента данных.

3. Односторонние функции не эквивалентны цифровым отпечаткам. Некоторые односторонние функции не подходят для создания цифровых отпечатков, а некоторые цифровые отпечатки создаются без использования односторонних функций.

4. Вычисление цифровой подписи с помощью асимметричного алгоритма может потребовать значительного времени, так как асимметричные алгоритмы, как правило, требуют многочисленных вычислений. Цифровая подпись может быть вычислена по цифровому отпечатку данных, а не по самим данным. Это может привести к повышению

эффективности, поскольку может оказаться быстрее вычислить цифровую подпись для короткого цифрового отпечатка, чем для длинного сообщения.

Криптографическое контрольное значение не обязательно защищает от воспроизведения единичного блока данных. Защиты от воспроизведения можно достичь включением в данные некоторой информации, которая может быть использована для выявления воспроизведения, например, порядкового номера или временной метки, или использованием криптографического зацепления. Чтобы обеспечить защиту от воспроизведения, информация должна быть проверена получателем защищенного блока данных.

8.3 Сертификаты безопасности

8.3.1 Введение в сертификаты безопасности

Сертификат безопасности представляет собой набор связанных с безопасностью данных, предоставленных уполномоченным по безопасности или доверенной третьей стороной, вместе с информацией безопасности, используемой при обеспечении для данных сервисов целостности и аутентификации источника данных. Сертификат безопасности содержит указание периодов времени, в течение которых данные остаются действительными.

Сертификаты безопасности используются для передачи информации безопасности от уполномоченного по безопасности (или доверенной третьей стороны) сущностям, которым эта информация требуется для выполнения функций безопасности. Сертификат безопасности может содержать информацию безопасности для нескольких сервисов безопасности.

Как описано в других Основах безопасности, сертификат безопасности может содержать ИБ, используемую для следующего:

– управления доступом;
– аутентификации;
– соблюдения целостности;
– соблюдения конфиденциальности;
– неотказуемости;
– аудита;
– управления ключами.

8.3.2 Верификация и сцепление сертификатов безопасности

Верификация сертификата безопасности заключается в проверке его целостности, подтверждении подлинности заявленной сущности, выпустившей сертификат безопасности, и проверке того, что эта сущность уполномочена создавать сертификаты безопасности. Эти операции могут потребовать представления дополнительной ИБ.

Если верификатор сертификата безопасности не обладает ИБ, требуемой для верификации сертификата безопасности, для предоставления необходимой ИБ может быть использован сертификат безопасности от другого уполномоченного по безопасности. Этот процесс может быть повторен для получения цепочки сертификатов безопасности. Они несут ИБ, которая предоставляет безопасный маршрут от известного уполномоченного по безопасности (т.е. того, для которого ИБ уже была установлена) до сущности, которой требуется сертифицированная ИБ.

Цепочку сертификатов безопасности следует использовать, только если она соответствует ограничениям, налагаемым всеми причастными политиками безопасности. Существования цепочки недостаточно. Цепочку следует использовать, только если подобное использование разрешено отношениями доверия между верификатором цепочки и уполномоченными по безопасности, создавшими сертификаты в цепочке, а также между этими уполномоченными по безопасности. Эти отношения определяются политикой безопасности верификатора цепочки сертификатов и политиками безопасности уполномоченных по безопасности. В частности, некоторым уполномоченным по безопасности доверено выпускать сертификаты безопасности для некоторых других уполномоченных по безопасности, в то время как некоторым другим доверено выпускать сертификаты безопасности только для сущностей, которые они администрируют.

8.3.3 Отзыв сертификатов безопасности

ИБ, содержащаяся в сертификате безопасности, может стать недействительной. Например, при компрометации закрытого ключа соответствующий открытый ключ больше не должен использоваться, и, следовательно, сертификаты безопасности, содержащие этот открытый ключ, должны быть отозваны.

Механизмы, которые могут быть использованы для отзыва сертификатов безопасности, включают **сертификаты отзыва и сертификаты списков отзыва.**

8.3.4 Повторное использование сертификатов безопасности

Некоторые сертификаты безопасности предназначены для использования с целью поддержки многократных взаимодействий, в то время как другие предназначены для однократного применения. Примером сертификата безопасности, предназначенного для многократного использования, служит сертификат аутентификации, определенный в *ИСО/МЭК 9594-8*. Примером сертификата безопасности, предназначенного для однократного применения, служит сертификат управления доступом, дающий право на однократный доступ. Сертификаты безопасности, предназначенные для однократного использования, могут содержать

информацию, предотвращающую их повторное использование (например, уникальный номер).

8.3.5 Структура сертификата безопасности

Общая форма сертификата безопасности содержит три компонента:

– информация, требуемая во всех сертификатах безопасности;

– информация безопасности, специфичная для одного или нескольких сервисов безопасности;

– информация для контроля или ограничения использования информации безопасности.

Информация, требуемая во всех сертификатах безопасности, подразделяется на две категории:

а) Информация, обеспечивающая как целостность, так и аутентификацию источника данных (например, криптографическое контрольное значение и указатели информации, которая будет использоваться для его верификации). Поскольку предоставляется сервис аутентификации источника данных, то должен предоставляться также указатель идентификатора заявленного источника сертификата безопасности (т.е. выпустившего уполномоченного органа).

б) Информация, по которой срок годности может быть идентифицирован (например, явный срок годности) или выведен (например, время создания и неявный срок годности). Это предотвращает неограниченное повторное использование сертификата безопасности, хотя сертификат безопасности в течение срока годности может использоваться многократно.

Информация для контроля или ограничения использования информации безопасности подразделяется на три категории:

а) Информация, используемая для защиты сертификата безопасности от несанкционированного использования

Примерами служат:

1) информация (например, отличительный идентификатор), идентифицирующая сущность или сущности, ИБ которых включена в сертификат безопасности;

2) информация, идентифицирующая сущности, которым разрешено использовать ИБ, содержащуюся в сертификате безопасности;

3) информация, контролирующая, сколько раз сертификат может использоваться;

4) информация, идентифицирующая политику безопасности, в рамках которой должен использоваться сертификат безопасности;

5) методы защиты и ассоциированные параметры, предназначенные для защиты сертификата безопасности от хищения (см. примеры в Приложении А);

6) информация, используемая для защиты от воспроизведения (например, уникальный номер или запрос).

б) Информация, которая может быть использована в целях аудита безопасности

Примеры включают:

1) ссылочный идентификатор сертификата безопасности (например, порядковый номер), уникальный для сертификата безопасности применительно ко всем сертификатам безопасности, выпущенным тем же уполномоченным по безопасности или агентом;

2) идентификатор (для целей аудита) сущности, для которой первоначально был выдан сертификат.

в) Информация, которая может быть использована в целях восстановления безопасности

Примеры включают:

1) ссылочный идентификатор сертификата безопасности, который может быть использован для отзыва конкретного сертификата безопасности;

2) идентификатор группы сертификатов безопасности, который может быть использован для отзыва группы сертификатов безопасности.

8.4 Маркеры безопасности

Маркеры безопасности могут быть классифицированы в соответствии с тем, кто их создал, и какие сервисы безопасности используются для защиты их содержимого.

Маркер безопасности, созданный уполномоченным по безопасности и защищенный сервисами целостности и аутентификации источника данных, называется сертификатом безопасности (см. 8.3).

Для многих механизмов безопасности необходим обмен информацией безопасности с защитой целостности между двумя взаимодействующими сущностями, ни одна из которых не является уполномоченным по безопасности. Маркеры безопасности, используемые для проведения таких обменов с защитой целостности, не являются сертификатами безопасности, поскольку сгенерировавшие их сущности не являются уполномоченными по безопасности. Такие маркеры безопасности называются **маркерами безопасности с защитой целостности.**

Все маркеры безопасности с защитой целостности содержат следующую информацию:

– информацию, обеспечивающую как целостность, так и аутентификацию источника данных (например, криптографическое контрольное значение и указатель информации, используемой для его верификации).

Все маркеры безопасности с защитой целостности содержат следующую информацию:

– информацию, по которой может быть определен срок годности;

– информацию, используемую для защиты от воспроизведения (например, уникальный номер).

9 Универсальные средства безопасности

Многие средства требуются более, чем в одной части Основ безопасности. В данном разделе определяются эти средства, предназначенные для использования в других частях Основ безопасности.

9.1 Средства, относящиеся к управлению

В этом подразделе идентифицируются универсальные типы средств управления. Могут существовать подклассы этих средств управления, специфичные для конкретных механизмов безопасности.

9.1.1 Инсталлировать ИБ.

Это средство устанавливает начальный набор ИБ, связанной с элементом.

9.1.2 Деинсталлировать ИБ.

Это средство вызывает удаление сущности из домена безопасности, отзывая ИБ, которая декларирует членство сущности в домене безопасности.

9.1.3 Изменить ИБ.

Это средство выполняет модификацию ИБ, связанной с элементом.

9.1.4 Утвердить ИБ.

Это средство связывает набор ИБ с элементом. Средство «утвердить ИБ» запускается уполномоченным по безопасности или его агентом.

9.1.5 Сделать ИБ недействительной.

Это средство блокирует любое использование ИБ, ассоциированной с элементом. Средство «сделать ИБ недействительной» запускается уполномоченным по безопасности или его агентом. ИБ, блокированная средством «сделать ИБ недействительной», может оставаться хранимой в системе для целей аудита и обеспечения того, что ИБ остается блокированной.

9.1.6 Выключить/включить сервис безопасности.

Эти средства выключают и снова включают заданные аспекты сервиса безопасности.

9.1.7 Зарегистрировать.

Это средство заставляет уполномоченного по безопасности записать некоторую информацию безопасности, ассоциированную с сущностью. Средство регистрации может быть вызвано сущностью, отличной от уполномоченного по безопасности. Например, сущность, желающая войти в домен безопасности, может использовать средство регистрации для

уведомления уполномоченного по безопасности о своем желании войти в домен безопасности.

9.1.8 Отменить регистрацию.

Это средство вызывает удаление элемента из домена безопасности и отзыв ассоциированной с ним ИБ. Это средство запускается уполномоченным по безопасности или его агентом. Политика безопасности может требовать, чтобы некоторые типы ИБ никогда не уничтожались.

9.1.9 Распространить ИБ.

Это средство используется уполномоченным по безопасности или его агентом, чтобы сделать элементы ИБ доступными для других сущностей.

9.1.10 Перечислить ИБ.

Это средство выдает список ИБ, связанной с данным элементом.

9.2 Средства, относящиеся к эксплуатации

9.2.1 Идентифицировать доверенных уполномоченных по безопасности.

Это средство идентифицирует уполномоченных по безопасности, являющихся доверенными в контексте политики безопасности для конкретных элементов и заданных действий безопасности (например, для предоставления ключей шифрования, сертификатов безопасности управления доступом или сертификатов безопасности аутентификации).

9.2.2 Идентифицировать правила безопасного взаимодействия.

Это средство идентифицирует используемые правила безопасного взаимодействия, что может достигаться с помощью предустановленной информации или с помощью переговоров между взаимосвязанными элементами доменов, как описано в 7.2.4.

Примечание. Правила безопасного взаимодействия устанавливаются соглашением между доменами безопасности, а не использованием данного средства. Данное средство определяет, какие из уже определенных правил безопасного взаимодействия применимы к конкретному действию.

9.2.3 Собрать ИБ.

Это средство собирает ИБ перед действием. Примерами подклассов данного средства являются:

- Управление доступом: Получить ИУД инициатора, Получить ИУД цели.
- Аутентификация: Собрать.

9.2.4 Сгенерировать ИБ.

Это средство генерирует ИБ для конкретного действия, связанного с безопасностью. ИБ может быть привязана к данным.

Примерами подклассов данного средства являются:

- Управление доступом: Привязать ИУД действия.
- Аутентификация: Сгенерировать.
- Неотказуемость: Сгенерировать свидетельство.

9.2.5 Верифицировать ИБ

Это средство верифицирует действительность ИБ, порожденной с помощью вызова средства сгенерировать ИБ. Средство «верифицировать ИБ» может само порождать ИБ, возвращаемую другому вызову средства верифицировать ИБ.

Примерами подклассов данного средства являются:

– Управление доступом: Верифицировать ИУД действия.

– Аутентификация: Верифицировать.

– Неотказуемость: Утвердить свидетельство.

Примером ситуации, в которой вывод средства верифицировать ИБ возвращается для дальнейшей верификации, является двусторонний протокол взаимной аутентификации. Предположим, что сущности А и В желают аутентифицировать друг друга, и А инициирует протокольный обмен. А вызывает средство сгенерировать для создания информации аутентификации, которая содержит и доказательство подлинности А, и запрос, на который, как ожидается, ответит В. В вызывает средство верифицировать для проверки того, что запрос получен от А, а также создает новый элемент информации аутентификации, содержащий доказательство подлинности В и ответ на запрос А. Затем А вызывает средство верифицировать для обработки ответа В. Средство верифицировать проверяет, что ответ получен от В, и что он соответствует первоначальному запросу.

10 Взаимодействие механизмов безопасности

Нередко для одного сеанса связи требуется несколько различных сервисов безопасности. Это требование может быть выполнено либо с помощью использования одного механизма безопасности, предоставляющего несколько сервисов безопасности, либо с помощью одновременного использования нескольких различных механизмов безопасности.

Иногда, при одновременном использовании различных механизмов безопасности, эти механизмы взаимодействуют вредоносным образом, что может эксплуатироваться атакующим. То есть, механизмы, обеспечивающие приемлемый уровень безопасности при использовании по отдельности, могут стать более уязвимыми при использовании в комбинации с другими механизмами. Нередко два механизма безопасности можно объединить несколькими различными способами; уязвимости объединенных механизмов могут различаться в зависимости от способа их объединения.

Особенно важный случай взаимодействия между механизмами встречается при объединении двух криптографических механизмов (например, механизма целостности и механизма конфиденциальности, или

механизма неотказуемости и механизма конфиденциальности). Свойства безопасности объединенных механизмов зависят от порядка, в котором применяются эти два криптографических преобразования.

В общем случае, при использовании асимметричных криптографических алгоритмов, преобразования целостности или неотказуемости следует применять к открытому тексту, а затем результирующие подписанные или опломбированные данные следует зашифровать.

Примером ситуации, в которой эти два сервиса необходимо применять в обратном порядке (т.е. сначала — сервис конфиденциальности) является случай, когда сервисы применяются между различными сущностями, и одна сущность должна иметь возможность верифицировать целостность зашифрованного текста при отсутствии разрешения знать открытый текст. Подобная ситуация может встречаться в системах обработки сообщений, когда агенту передачи сообщений может потребоваться проверить целостность и источник сообщения при отсутствии разрешения знать, каков открытый текст сообщения.

Использование сервисов конфиденциальности и целостности в обратном порядке несет в себе риск того, что сервис целостности не сможет поддержать неотказуемость. Если нужны все три сервиса, и необходим обратный порядок целостности и конфиденциальности, то можно применить два механизма целостности, один перед применением механизма конфиденциальности, а другой – после. Пример подобной ситуации встречается в системах обработки сообщений; при обеспечении конфиденциальности в сообщении можно использовать две различных цифровых подписи (одна вычисляется для зашифрованного текста и используется агентом передачи сообщений, а другая вычисляется для открытого текста, обеспечивая для получателя неотказуемость отправителя).

11 Отказ в обслуживании и доступность

Отказ в обслуживании возникает всякий раз, когда значения параметров обслуживания падают ниже требуемого уровня, включая случаи, когда сервис становится недоступным. Подобный отказ в обслуживании может быть вызван намеренной атакой или случайными обстоятельствами, такими как буря или землетрясение. Доступность — это условие отсутствия отказа в обслуживании или деградации качества коммуникаций.

Не всегда возможно предотвратить условие отказа в обслуживании. Для выявления отказа в обслуживании могут использоваться сервисы безопасности, что позволяет принять корректирующие меры. При подобном выявлении не всегда можно определить, было ли это условие результатом атаки или случайных обстоятельств. Конкретная политика безопасности

может требовать, что при выявлении условия отказа в обслуживании это следует запротоколировать (для целей аудита) и послать сигнал тревоги процессору сигналов тревоги.

Как только выявляется условие отказа в обслуживании, сервисы безопасности могут также использоваться для исправления ситуации и возвращения к приемлемому уровню обслуживания. Это выявление и корректирующие действия могут включать использование сервисов безопасности и других сервисов (например, маршрутизацию трафика по другим каналам, переключение на резервные средства хранения или включение резервных процессоров).

Атаки типа «отказ в обслуживании» могут быть направлены на множество различных типов сервисов, и механизмы, используемые для предотвращения таких атак, могут варьироваться в зависимости от типа защищаемого приложения. Это означает, что невозможно ввести общую классификацию механизмов, защищающих от отказа в обслуживании, и, следовательно, описание отдельных инфраструктур безопасности не будет более затрагивать эти механизмы.

12 Прочие требования

Могут потребоваться меры безопасности помимо описанных в этих частях Основ (например, меры физической безопасности и безопасности персонала). Определение сервисов безопасности для поддержки подобных мер выходит за рамки настоящего стандарта. Использование подобных дополнительных мер безопасности может даже устранить необходимость в некоторых сервисах безопасности, описанных в этих Основах.

Приложение А
(справочное)
Некоторые примеры механизмов защиты сертификатов безопасности

Потенциальная угроза сертификатам безопасности - это угроза того, что атакующий ложно объявит себя сущностью, на которую ссылается сертификат безопасности. Подобное несанкционированное использование сертификата безопасности называется кражей сертификата безопасности.

Эта угроза может быть как внешней, так и внутренней. Внешняя угроза состоит в том, что атакующий может получить сертификат безопасности, прослушивая коммуникации, к которым он иным образом не может подключиться. Внутренняя угроза состоит в том, что сущность, имеющая законную необходимость получить сертификат (например, для того, чтобы установить ИБ сущности, с которой она взаимодействует), может ложно объявить себя сущностью, фигурирующей в сертификате.

Сертификат безопасности может быть защищен от кражи путем непосредственного использования сервисов безопасности коммуникаций ВОС или с помощью альтернативного метода защиты, требующего дополнительных параметров, внутренних и внешних для сертификата безопасности.

Механизм защиты сертификатов безопасности поддерживает делегирование, если сущность, имеющая право использовать сертификат безопасности, может передать это право другой сущности. Некоторые из механизмов, описанных в данном приложении, поддерживают делегирование.

А.1 Защита с использованием сервиса безопасности коммуникаций ВОС

Угрозе кражи со стороны внешнего злоумышленника можно противостоять путем использования сервиса конфиденциальности при передаче сертификата безопасности между взаимодействующими сущностями.

А.2 Защита с помощью внутреннего параметра сертификата безопасности

Существует множество альтернативных методов защитить сертификаты безопасности от кражи. Каждый из этих методов полагается на внутренние параметры в сертификате и ассоциированные внешние параметры. Конкретные используемые методы могут быть указаны в сертификате безопасности.

Эти методы включают:

- метод аутентификации;
- метод секретного ключа;
- метод открытого ключа;
- метод односторонней функции.

Сертификат безопасности может использовать комбинацию нескольких из этих методов.

А.2.1 Метод аутентификации.

В этом методе внутренним параметром являются отличительные идентификаторы сущностей, которым разрешено использовать сертификат. Внешним параметром является отличительный идентификатор сущности, которая пытается использовать сертификат. Этот внешний параметр предоставляется сервисом аутентификации. Кроме того, сертификат может включать дополнительные параметры, такие как порядковый номер сертификата безопасности, который должен использоваться процессом аутентификации.

Метод аутентификации обеспечивает следующую защиту сертификата безопасности:

- Он ограничивает использование сертификата безопасности только сущностями, идентификаторы которых включены в сертификат безопасности.

Этот метод не разрешает уполномоченному пользователю сертификата передавать это право другой сущности, так как набор сущностей, которые могут использовать сертификат, фиксируется в момент создания сертификата. То есть, этот метод не поддерживает делегирование.

А.2.2 Метод секретного ключа.

В этом методе весь сертификат зашифровывается с помощью симметричного криптографического алгоритма. Внешним параметром в этом методе является секретный ключ, который был использован для зашифрования сертификата.

Метод секретного ключа обеспечивает следующую защиту сертификата безопасности:

- он ограничивает использование сертификата безопасности только сущностями, которым известно значение секретного ключа (и которые, следовательно, могут расшифровать зашифрованный сертификат).

Этот метод поддерживает делегирование, так как уполномоченный пользователь сертификата может передать это право другой сущности, передав ей либо секретный ключ, либо расшифрованный сертификат.

А.2.3 Метод открытого ключа.

В этом методе внутренним параметром является открытый ключ. Внешним параметром является соответствующий закрытый ключ.

Метод открытого ключа обеспечивает следующую защиту сертификата безопасности:

- он ограничивает использование сертификата безопасности только сущностями, которым известно значение закрытого ключа (и которые, следовательно, могут вычислить цифровые подписи с использованием закрытого ключа).

Этот метод поддерживает делегирование, так как уполномоченный пользователь сертификата может передать это право другой сущности, передав ей закрытый ключ.

А.2.4 Метод односторонней функции.

В этом методе внутренним параметром является результат применения односторонней функции к внешнему параметру. Внутренний параметр называется ключом защиты, в то время как внешний параметр называется контрольным ключом.

Метод односторонней функции обеспечивает следующую защиту сертификата безопасности:

-он ограничивает использование сертификата безопасности только сущностями, которым известно значение контрольного ключа (и которые, следовательно, могут доказать, что им известен контрольный ключ, раскрыв его значение).

Этот метод поддерживает делегирование, так как уполномоченный пользователь сертификата может передать это право другой сущности, передав ей контрольный ключ.

А.3 Защита внешних и внутренних параметров при передаче

Рассматриваются четыре случая:

- Передача внутреннего параметра центру выпуска сертификатов перед созданием сертификата. Это требуется, только если внутренние и внешние параметры не генерируются центром выпуска сертификатов.

- Передача внешнего параметра центром выпуска сертификатов после создания сертификата. Это требуется, только если внутренние и внешние параметры генерируются центром выпуска сертификатов.

- Передача внешнего параметра между сущностями при подтверждении права использовать сертификат.

- Передача внешнего параметра между сущностями при делегировании права использовать сертификат.

А.3.1 Передача внутренних параметров центру выпуска сертификатов.

В методе аутентификации, методе открытого ключа и методе односторонней функции перед внесением в сертификат безопасности внутренний параметр может быть сообщен уполномоченному по безопасности. При передаче внутреннего параметра уполномоченному по безопасности его целостность должна быть защищена.

В методе секретного ключа перед созданием сертификата безопасности внешний параметр (т.е. секретный ключ) может быть сообщен уполномоченному по безопасности. При этой передаче требуется защита как целостности, так и конфиденциальности.

А.3.2 Передача внешних параметров между сущностями.

В методе аутентификации внешний параметр (идентификатор пользователя сертификата) предоставляется механизмом аутентификации.

В методе секретного ключа и методе односторонней функции внешний параметр должен передаваться между сущностями при использовании сертификата. Это ограничивает использование сертификата безопасности теми, кому известно правильное значение секретного ключа или контрольного ключа. При передаче внешнего параметра между сущностями его конфиденциальность должна быть защищена.

Различие между двумя методами состоит в том, что при использовании метода секретного ключа необходимо раскрыть значение внешнего параметра до того, как можно будет проверить криптографическое контрольное значение сертификата безопасности, в то время как в методе односторонней функции контрольное значение сертификата безопасности может быть проверено перед раскрытием внешнего параметра.

В методе закрытого ключа внешний параметр не нужно передавать между сущностями при использовании сертификата, так как сущность может доказать, что ей известен закрытый ключ, не раскрывая его (создав цифровую подпись). В этом методе внешний параметр (закрытый ключ) нужно передавать только при делегировании права использования сертификата. При передаче закрытого ключа между сущностями его конфиденциальность должна быть защищена.

А.4 Использование сертификатов безопасности отдельными сущностями или группами сущностей

Описанные выше методы защиты могут быть использованы для ограничения использования сертификата безопасности либо одной поименованной сущностью, либо поименованной группой сущностей:

- Сертификат безопасности может быть связан с конкретной сущностью; секретный ключ, закрытый ключ или контрольный ключ передается единственной сущности в зашифрованном виде, и в сертификате появляются отличительный идентификатор или атрибуты безопасности данной сущности.

- Сертификат безопасности может быть связан с поименованной группой сущностей; секретный ключ, закрытый ключ или контрольный ключ передается членам группы в зашифрованном виде, и в сертификате появляются отличительный идентификатор или атрибуты безопасности группы. Таким образом, любой член группы может использовать сертификат безопасности.

А.5 Связывание сертификата безопасности с доступами

Сертификаты безопасности могут использоваться для управления доступом. В этом случае важно установить защищенную связь между сертификатом безопасности и запросами доступа, которые он поддерживает. Если такой защищенной связи нет, то сертификат безопасности уязвим относительно атаки воспроизведением, в которой

атакующий передает копию подлинного сертификата безопасности для подделки запроса доступа.

Эта атака может быть предотвращена с помощью использования сервиса целостности для связывания вместе сертификата безопасности, внешнего параметра и запроса доступа.

При использовании метода аутентификации эта связь может быть получена с помощью связывания обмена информацией аутентификации с механизмом целостности, как описано в Основах аутентификации (см. *СТ РК ИСО/МЭК 10181-2-2008).*

При использовании метода секретного ключа эта привязка может быть получена с помощью включения ключа механизма целостности в тело сертификата безопасности и использования этого ключа для опломбирования запроса доступа. Или же в качестве ключа механизма целостности может быть использован секретный ключ (либо его разновидность).

Примечание. Использование одного криптографического ключа и для механизма целостности, и для механизма конфиденциальности может сделать возможными некоторые виды атак. Чтобы избежать этой угрозы могут быть использованы варианты ключа. Вариант криптографического ключа – это другой криптографический ключ, полученный из первоначального ключа, но не являющийся им.

При использовании метода односторонней функции эта привязка может быть получена путем использования контрольного ключа в качестве ключа механизма целостности, основанного на односторонних функциях.

При использовании метода открытого ключа эта привязка может быть получена путем использования закрытого ключа для подписывания запросов доступа.

Во всех этих методах связывание сертификата безопасности, внешнего параметра и запроса доступа может быть также получено путем использования сервиса целостности, который предоставляется как часть сервиса коммуникаций ВОС.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, взаимодействие сетей, взаимодействие открытых систем, коммуникационные процедуры, защита информации, технологии безопасности, обзор.

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074